CHAPTER 37

QoS の設定

この章では、自動 Quality of Service（QoS）コマンドを使用して、またはスイッチで標準の QoS コマンドを使用して QoS を設定する方法について説明します。QoS を使用すると、特定の種類のトラフィックを他のトラフィックよりも優先的に処理できます。QoS を使用しなかった場合、スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供します。信頼性、遅延限度、またはスループットに関して保証することなく、スイッチはパケットを送信します。特に記述がない限り、*スイッチ*という用語はスタンドアロン スイッチとスイッチ スタックを意味しています。

Cisco IOS Release 12.2(52)SE 以降のリリースでは、デュアル IPv4/IPv6 SDM テンプレートが設定されている場合、IPv4 および IPv6 の両方のトラフィックの QoS をサポートします。

QoS は物理ポート、および Switch Virtual Interfaces（SVI; スイッチ仮想インターフェイス）で設定できます。ポリシー マップを適用するほかに、分類、キューイング、スケジューリングなどの QoS を同じ方法で物理ポートまたは SVI に設定します。物理ポートに QoS を設定すると、非階層型ポリシー マップが適用されます。SVI に QoS を設定すると、非階層型または階層型ポリシー マップが適用されます。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

スイッチは、Modular QoS Command Line Interface（MQC; モジュラ QoS コマンドライン インターフェイス）コマンドの一部をサポートします。MQC コマンドの詳細については、次の URL にアクセスし、「Modular Quality of Service Command-Line Interface Overview」を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800bd908.html9

QoS の概要

ネットワークは通常、ベストエフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、正しいタイミングで配信される可能性も同じです。輻輳が発生した場合に、ドロップされる可能性についても、すべてのトラフィックで同じです。

QoS 機能を設定すると、特定のネットワーク トラフィックを選択し、相対的な重要性に応じてそのトラフィックにプライオリティを指定し、輻輳管理および輻輳回避技術を使用して、優先処理を実行できます。ネットワークに QoS を実装すると、ネットワーク パフォーマンスがさらに予測しやすくなり、帯域幅をより効率的に利用できるようになります。

QoS は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）の新しい規格である Differentiated Services（DiffServ; 差別化サービス）アーキテクチャに基づいて実装されます。このアーキテクチャでは、ネットワークに入るときに各パケットを分類することが規定されています。

この分類は IP パケット ヘッダーに格納され、推奨されない IP Type of Service（ToS; サービス タイプ）フィールドの 6 ビットを使用して、分類（クラス）情報として伝達されます。分類情報はレイヤ 2 フレームで伝達することもできます。ここでは、レイヤ 2 フレームまたはレイヤ 3 パケット内のこれらの特殊ビットについて説明します（図 37-1 を参照）。

- レイヤ 2 フレームのプライオリティ ビット

  レイヤ 2 802.1Q フレーム ヘッダーには、2 バイトのタグ制御情報フィールドがあり、上位 3 ビット（ユーザ プライオリティ ビット）で CoS 値が伝達されます。レイヤ 2 802.1Q トランクとして設定されたポートでは、ネイティブ VLAN（バーチャル LAN）のトラフィックを除くすべてのトラフィックが 802.1Q フレームに収められます。

  他のフレーム タイプでレイヤ 2 CoS 値を伝達することはできません。

  レイヤ 2 CoS 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

- レイヤ 3 パケットのプライオリティ ビット

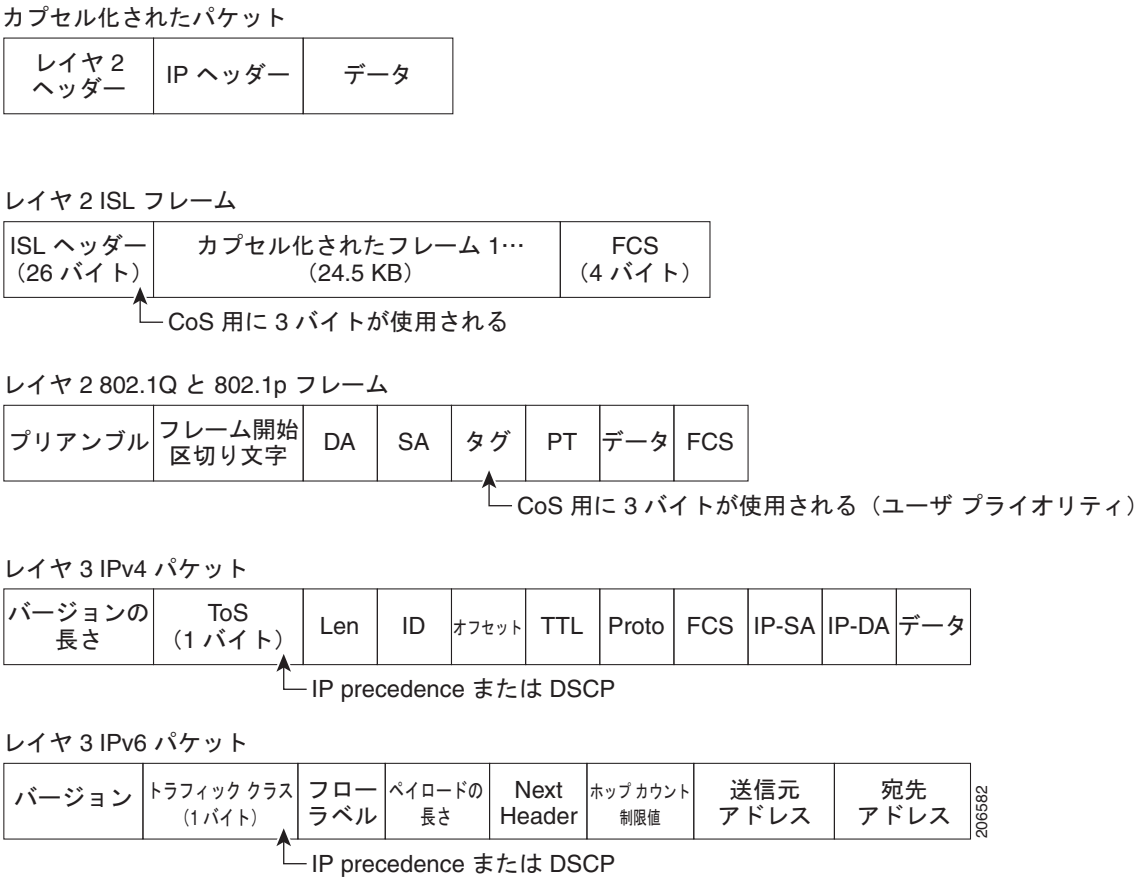
  レイヤ 3 IP パケットは、IP precedence 値または Differentiated Services Code Point（DSCP; Diffserv コード ポイント）値のいずれかを伝達します。DSCP 値は IP precedence 値と下位互換性があるため、QoS ではどちらの値も使用できます。

  IP precedence 値の範囲は 0 ～ 7 です。

  DSCP 値の範囲は 0 ～ 63 です。

（注）Cisco IOS Release 12.2(52)SE 以降から、デュアル IPv4/IPv6 SDM テンプレートを使用して、スイッチまたはスイッチ スタックでグローバルに IPv6 QoS をイネーブルにできるようになりました。デュアル IPv4 および IPv6 テンプレートを設定したらスイッチをリロードする必要があります。詳細については、第 8 章「SDM テンプレートの設定」を参照してください。

図 37-1　フレームおよびパケットにおける QoS 分類レイヤ



インターネットにアクセスするすべてのスイッチおよびルータはクラス情報に基づいて、同じクラス情報が与えられているパケットは同じ扱いで転送を処理し、異なるクラス情報のパケットはそれぞれ異なる扱いをします。パケットのクラス情報は、設定されているポリシー、パケットの詳細な検証、またはその両方に基づいて、エンド ホストが割り当てるか、または伝送中にスイッチまたはルータで割り当てることができます。パケットの詳細な検証は、コア スイッチおよびルータの負荷が重くならないように、ネットワークのエッジ付近で行います。

パス上のスイッチおよびルータは、クラス情報を使用して、個々のトラフィック クラスに割り当てるリソースの容量を制限できます。DiffServ アーキテクチャでトラフィックを処理するときの、各デバイスの動作をホップ単位動作といいます。パス上のすべてのデバイスに一貫性のあるホップ単位動作をさせることによって、エンドツーエンドの QoS ソリューションを構築できます。

ネットワークに QoS を実装する作業は、インターネットワーキング デバイスによって提供される QoS の機能、ネットワーク内のトラフィック タイプとパターン、および着信 / 発信トラフィックに必要な制御の細かさによって、難易度が変化します。

QoS の基本モデル

QoS を実装するには、スイッチ上でパケットまたはフローを相互に区別（分類）し、パケットがスイッチを通過するときに所定の Quality of Service を示すラベルを割り当て、設定されたリソース使用率制限にパケットを適合させ（ポリシングおよびマーキング）、リソース競合の発生状況に応じて異なる処理（キューイングおよびスケジューリング）を行う必要があります。また、スイッチが送信するトラフィックが特定のトラフィック プロファイルを満たすようにする必要もあります（シェーピング）。

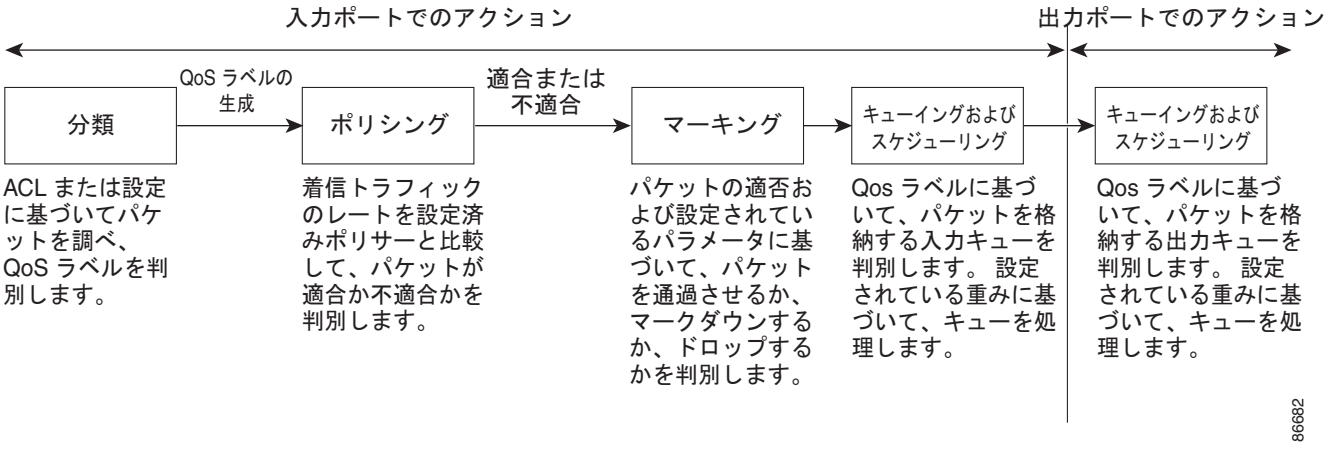
図 37-2 に、QoS の基本モデルを示します。入力ポートでのアクションには、トラフィックの分類、ポリシング、マーキング、キューイング、およびスケジューリングがあります。

- 分類は、QoS ラベルを対応付けて、パケットごとに異なるパスを生成するプロセスです。スイッチはパケット内の CoS または DSCP を QoS ラベルにマッピングして、トラフィックの種類を区別します。生成された QoS ラベルは、このパケットでこれ以降に実行されるすべての QoS アクションを識別します。詳細については、「分類」（P.37-5）を参照してください。
- ポリシングでは、着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不適合かを判別します。ポリサーは、トラフィック フローで消費される帯域幅を制限します。その判別結果がマーカーに渡されます。詳細については、「ポリシングおよびマーキング」（P.37-9）を参照してください。
- マーキングでは、ポリサーおよびパケットが不適合である場合の対処法に関する設定情報を評価します。また、パケットに関する処理内容（変更しないでパケットを通過させるか、パケットの QoS ラベルをマークダウンするか、またはパケットをドロップするか）を決定します。詳細については、「ポリシングおよびマーキング」（P.37-9）を参照してください。
- キューイングでは、QoS ラベルおよび対応する DSCP または CoS 値を評価して、パケットを 2 つの入力キューのどちらに格納するかを選択します。キューイングは、輻輳回避メカニズムである Weighted Tail Drop（WTD）アルゴリズムによって拡張されます。しきい値を超過している場合、パケットはドロップされます。詳細については、「キューイングおよびスケジューリングの概要」（P.37-14）を参照してください。
- スケジューリングでは、設定されている Shaped Round Robin（SRR）の重みに基づいて、キューを処理します。入力キューの 1 つがプライオリティ キューです。共有が設定されている場合、SRR はプライオリティ キューを処理してから他のキューを処理します。詳細については、「SRR のシェーピングおよび共有」（P.37-15）を参照してください。

出力ポートでのアクションには、キューイングおよびスケジューリングがあります。

- キューイングでは、QoS パケット ラベルおよび対応する DSCP または CoS 値を評価して、4 つの出力キューのどれを使用するかを選択します。複数の入力ポートが 1 つの出力ポートに同時にデータを送信すると輻輳が発生することがあるため、WTD を使用してトラフィック クラスを区別し、QoS ラベルに基づいてパケットごとに異なるしきい値を適用します。しきい値を超過している場合、パケットはドロップされます。詳細については、「キューイングおよびスケジューリングの概要」（P.37-14）を参照してください。
- スケジューリングでは、設定されている SRR の共有重みまたはシェーピング重みに基づいて、4 つの出力キューを処理します。キューの 1 つ（キュー 1）は、他のキューの処理前に空になるまで処理される緊急キューにすることができます。

図 37-2　QoS の基本モデル



分類

分類とは、パケットのフィールドを検証して、トラフィックのタイプを区別するプロセスです。QoS がスイッチ上でグローバルにイネーブルになっている場合だけ、分類はイネーブルです。デフォルトでは、QoS はグローバルにディセーブルになっているため、分類は実行されません。

分類中に、スイッチは検索処理を実行し、パケットに QoS ラベルを割り当てます。QoS ラベルは、パケットに対して実行するすべての QoS アクション、およびパケットの送信元キューを識別します。

QoS ラベルは、パケット内の DSCP または CoS 値に基づいて、パケットに実行されるキューイングおよびスケジューリング アクションを判別します。QoS ラベルは信頼設定およびパケット タイプに従ってマッピングされます（図 37-3（P.37-7）を参照）。

着信トラフィックを分類するには、フレームまたはパケット内のどのフィールドを使用するかを指定します。非 IP トラフィックの場合は、次の方法で分類を実行できます（図 37-3 を参照）。

- 着信フレーム内の CoS 値を信頼します（CoS を信頼するようにポートを設定します）。次に、設定可能な CoS/DSCP マップを使用して、パケットの DSCP 値を生成します。レイヤ 2 802.1Q フレームのヘッダーは、タグ制御情報フィールドの上位 3 ビットで CoS 値を伝達します。CoS 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。
- 着信フレームの DSCP または IP precedence 値を信頼します。これらの設定は、非 IP トラフィックの場合は無意味です。これらのいずれかの方法で設定されているポートに非 IP トラフィックが着信した場合は、CoS 値が割り当てられ、CoS/DSCP マップから内部 DSCP 値が生成されます。スイッチは内部 DSCP 値を使用して、トラフィックのプライオリティを表示する CoS 値を生成します。
- 設定されたレイヤ 2 の MAC Access Control List（ACL; アクセス コントロール リスト）に基づいて分類します。レイヤ 2 の MAC ACL では、MAC 送信元アドレス、MAC 宛先アドレス、およびその他のフィールドを調べることができます。ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。ACL が設定されている場合は、ポリシーマップ アクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

IP トラフィックの場合は、次の方法で分類を実行できます（図 37-3 を参照）。

- 着信パケットの DSCP 値を信頼し（DSCP を信頼するようにポートを設定）、パケットに同じ DSCP 値を割り当てます。IETF では、1 バイトの ToS フィールドの上位 6 ビットが DSCP として定義されています。特定の DSCP 値が表すプライオリティは、設定可能です。DSCP 値の範囲は 0 ～ 63 です。

  2 つの QoS 管理ドメインの境界上にあるポートの場合は、設定可能な DSCP/DSCP 変換マップを使用し、DSCP を別の値に変更することができます。

  Cisco IOS Release 12.2(52)SE 以降のリリースでは、IPv6 DSCP に基づいて IP トラフィックを分類するオプションがあります。

- 着信パケットの IP precedence 値を信頼し（IP precedence を信頼するようにポートを設定し）、設定可能な IP precedence/DSCP マップを使用してパケットの DSCP 値を生成します。IP Version 4 仕様では、1 バイトの ToS フィールドの上位 3 ビットが IP precedence として定義されています。IP precedence 値の範囲は 0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

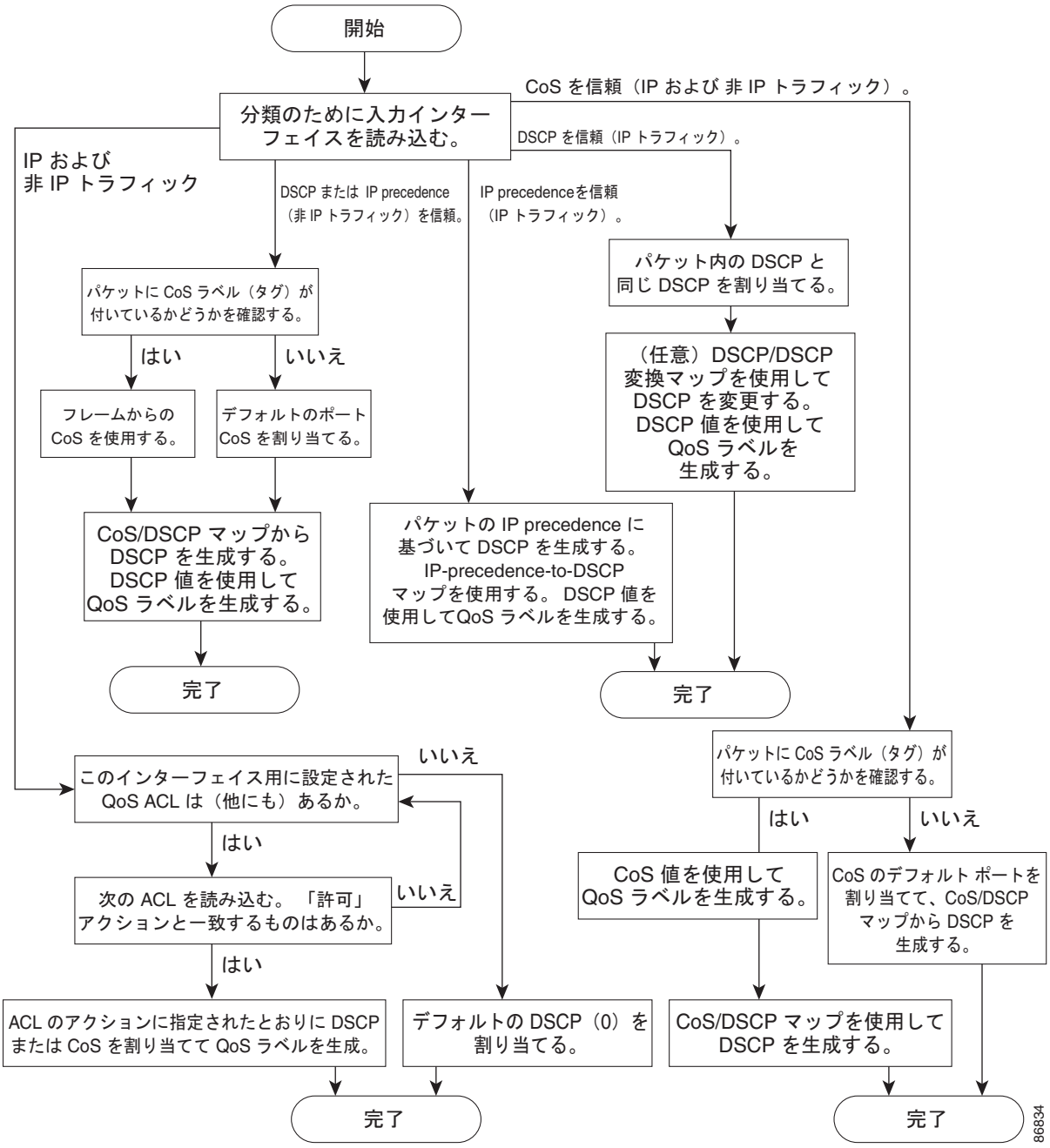
  Cisco IOS Release 12.2(52)SE 以降のリリースでは、IPv6 IP precedence に基づいて IP トラフィックを分類するオプションがあります。

- 着信パケットに CoS 値がある場合にはこれを信頼し、CoS/DSCP マップを使用してパケットの DSCP 値を生成します。CoS 値が存在しない場合は、デフォルトのポート CoS 値を使用します。
- 着信パケットの設定された CoS を上書きして、これらにデフォルトのポート CoS 値を適用します。IPv6 パケットの場合、DSCP 値は CoS/DSCP マップおよびデフォルトのポート CoS 値を使用して書き換えられます。Cisco IOS Release 12.2(52)SE 以降のリリースでは、これを IPv4 および IPv6 の両方トラフィックで実行できます。
- 設定された IP 標準 ACL または IP 拡張 ACL（IP ヘッダーの各フィールドを調べる）に基づいて、分類を実行します。ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。ACL が設定されている場合は、ポリシーマップ アクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

ここで説明されているマップの詳細については、「マッピング テーブル」（P.37-13）を参照してください。ポートの信頼状態の設定情報については、「ポートの信頼状態を使用した分類の設定」（P.37-42）を参照してください。

分類が行われたパケットは、ポリシング、マーキング、および入力キューイングとスケジューリングの各段階に送られます。

図 37-3　分類のフローチャート



QoS ACL に基づく分類

IP 標準 ACL、IP 拡張 ACL、またはレイヤ 2 MAC ACL を使用すると、同じ特性を備えたパケット グループ（クラス）を定義できます。Cisco IOS Release 12.2(52)SE 以降のリリースでは、IPv6 ACL に基づいて IP トラフィックを分類できます。QoS のコンテキストでは、Access Control Entry（ACE; アクセス コントロール エントリ）の許可および拒否アクションの意味が、セキュリティ ACL の場合とは異なります。

- 許可アクションとの一致が検出されると（最初の一致の原則）、指定の QoS 関連アクションが実行されます。
- 拒否アクションと一致した場合は、処理中の ACL が省略され、次の ACL が処理されます。
- 許可アクションとの一致が検出されないまま、すべての ACE の検証が終了した場合、そのパケットでは QoS 処理は実行されず、ベストエフォート型サービスが実行されます。
- ポートに複数の ACL が設定されている場合に、許可アクションを含む最初の ACL とパケットの一致が見つかると、それ以降の検索処理は中止され、QoS 処理が開始されます。

（注）アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

ACL を使用して定義されたトラフィック クラスには、ポリシーを付加できます。ポリシーにはそれぞれにアクションを指定した複数のクラスを含めることができます。ポリシーには、クラスを特定のグループとして分類する（たとえば DSCP を割り当てる）コマンドや、クラスの速度制限を行うコマンドが含まれます。このポリシーを特定のポートに結合すると、そのポートでポリシーが有効になります。

IP ACL を実装して IP トラフィックを分類する場合は、**access-list** グローバル コンフィギュレーション コマンドを使用します。レイヤ 2 MAC ACL を実装して非 IP トラフィックを分類する場合は、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。設定情報については、「QoS ポリシーの設定」（P.37-49）を参照してください。

クラス マップおよびポリシー マップに基づく分類

クラス マップは、特定のトラフィック フロー（またはクラス）に名前を付けて、他のすべてのトラフィックと区別するためのメカニズムです。クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。この条件には、ACL で定義されたアクセス グループとの照合、または DSCP 値や IP precedence 値の特定のリストとの照合を含めることができます。複数のトラフィック タイプを分類する場合は、別のクラス マップを作成し、異なる名前を使用できます。パケットをクラス マップ条件と照合した後で、ポリシー マップを使用してさらに分類します。

ポリシー マップでは、作用対象のトラフィック クラスを指定します。アクションには、トラフィック クラスの CoS、DSCP、または IP precedence 値を信頼するアクション、トラフィック クラスに特定の DSCP または IP precedence 値を設定するアクション、またはトラフィック帯域幅の制限およびトラフィックが不適合な場合の対処方法を指定するアクションなどを指定できます。ポリシー マップを効率的に機能させるには、ポートにポリシー マップを結合しなければなりません。

クラス マップを作成するには、**class-map** グローバル コンフィギュレーション コマンドまたは **class** ポリシー マップ コンフィギュレーション コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用します。**class-map** コマンドを入力すると、クラス マップ コンフィギュレーション モードが開始されます。このモードで、**match** クラス マップ コンフィギュレーション コマンドを使用して、トラフィックの一致条件を定義します。

class class-default ポリシー マップ コンフィギュレーション コマンドを使用して、デフォルト クラスを設定できます。未分類のトラフィック（トラフィック クラスに指定された一致基準を満たさないラフィック）は、デフォルトのトラフィックとして処理されます。

ポリシー マップは、**policy-map** グローバル コンフィギュレーション コマンドを使用して作成し、名前を付けます。このコマンドを入力すると、ポリシー マップ コンフィギュレーション モードが開始されます。このモードでは、**class**、**trust**、または **set** ポリシー マップ コンフィギュレーション コマンドおよびポリシー マップ クラス コンフィギュレーション コマンドを使用して、特定のトラフィック クラスに対して実行するアクションを指定します。

ポリシー マップには、ポリサー、トラフィックの帯域幅限度、および限度を超えた場合のアクションを定義する **police** および **police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドを含めることもできます。

ポリシー マップをイネーブルにするには、**service-policy** インターフェイス コンフィギュレーション コマンドを使用してポートにマップを結合します。

非階層型ポリシー マップは、物理ポートまたは SVI に適用できます。ただし、階層型ポリシー マップを適用できるのは、SVI だけです。階層ポリシー マップには 2 つのレベルがあります。1 番めは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。2 番めはインターフェイス レベルで、SVI の物理ポートのトラフィックに対して実行するアクションを指定します。インターフェイス レベルのアクションはインターフェイス レベルのポリシー マップで指定されます。

詳細については、「ポリシングおよびマーキング」（P.37-9）を参照してください。設定情報については、「QoS ポリシーの設定」（P.37-49）を参照してください。

ポリシングおよびマーキング

パケットを分類して、DSCP ベースまたは CoS ベースの QoS ラベルを割り当てた後で、ポリシングおよびマーキング プロセスを開始できます（図 37-4 を参照）。

ポリシングには、トラフィックの帯域幅限度を指定するポリサーの作成が伴います。この限度を超えたパケットは、*アウト オブ プロファイル*または*不適合*パケットです。各ポリサーは、パケットが適合であるかまたは不適合であるかをパケットごとに判別し、パケットに対するアクションを指定します。これらのアクションはマーカーによって実行されます。パケットを変更しないで通過させるアクション、パケットをドロップするアクション、またはパケットに割り当てられた DSCP 値を変更（マークダウン）してパケットの通過を許可するアクションなどがあります。設定可能なポリシング済み DSCP マップを使用すると、パケットに新しい DSCP ベース QoS ラベルが設定されます。ポリシング済み DSCP マップの詳細については、「マッピング テーブル」（P.37-13）を参照してください。マークダウンされたパケットは、元の QoS ラベルと同じキューを使用して、フロー内のパケットの順番が崩れないようにします。

（注）すべてのトラフィックは、ブリッジングされるかまたはルーティングされるかに関係なく、設定されている場合そのポリサーの影響を受けます。その結果、ブリッジングされたパケットは、ポリシングまたはマーキングが行われたときにドロップされたり、DSCP または CoS フィールドが変更されたりすることがあります。

物理ポートまたは SVI 上でポリシング（個別ポリサーまたは集約ポリサー）を設定できます。物理ポートのポリシング設定の詳細については、「物理ポートのポリシング」（P.37-10）を参照してください。SVI でポリシー マップを設定したら、階層型ポリシーマップを作成し、セカンダリ インターフェイス レベルのポリシー マップだけで個々のポリシーを定義できます。詳細については、「SVI のポリシング」（P.37-11）を参照してください。

ポリシー マップおよびポリシング アクションを設定した後で、**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、ポリシーを入力ポートまたは SVI に付加します。設定情報については、「ポリシー マップを使用した物理ポートのトラフィックの分類、ポリシング、およびマーキング」（P.37-61）、「階層型ポリシー マップを使用した SVI のトラフィックの分類、ポリシング、およびマーキング」（P.37-66）、および「集約ポリサーを使用したトラフィックの分類、ポリシング、およびマーキング」（P.37-74）を参照してください。

物理ポートのポリシング

物理ポートのポリシー マップでは、次のタイプのポリサーを作成できます。

- 個々の QoS はポリサーに指定された帯域幅限度を、一致したトラフィック クラスごとに別々に適用します。このタイプのポリサーは、**police** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップの中で設定します。
- 集約 QoS はポリサーで指定された帯域幅限度を、一致したすべてのトラフィック フローに累積的に適用します。このタイプのポリサーは、**police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップ内で集約ポリサー名を指定することにより設定します。ポリサーの帯域幅限度を指定するには、**mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。このようにして、集約ポリサーはポリシー マップ内にある複数のトラフィック クラスで共有されます。

（注）　SVI には個別のポリサーだけを設定します。

ポリシングはトークンバケット アルゴリズムを使用します。各フレームがスイッチに着信すると、バケットにトークンが追加されます。バケットは内部にホールがあり、平均トラフィック レートとしてビット/秒で指定されたレートで通過します。バケットにトークンが追加されるたびに、スイッチは、バケット内に十分なスペースがあるかを確認します。十分なスペースがなければ、パケットは不適合とマーキングされ、指定されたポリサー アクション（ドロップまたはマークダウン）が実行されます。

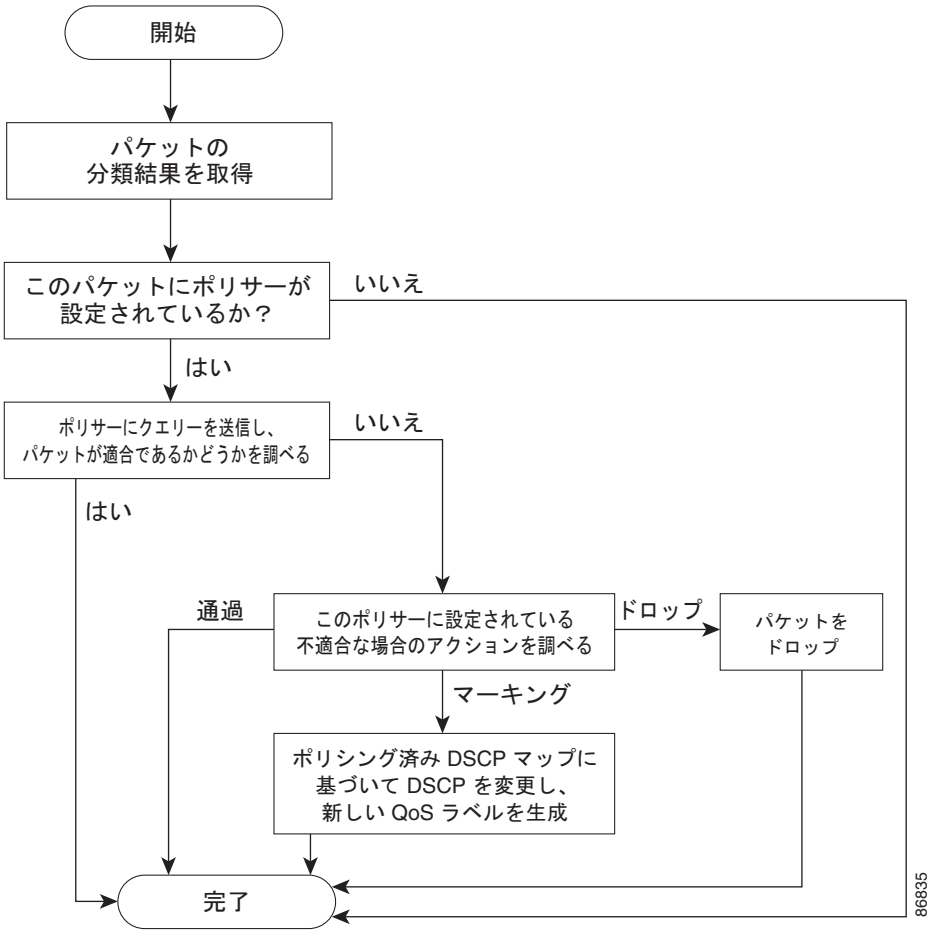
バケットが満たされる速度は、バケット深度（burst-byte）、トークンが削除されるレート（rate-bps）、および平均レートを上回るバースト期間によって決まります。バケットのサイズにより、バースト長に上限が設定され、バックツーバックで送信できるフレーム数が決まります。バースト期間が短い場合、バケットはオーバーフローせず、トラフィック フローに何のアクションも実行されません。ただし、バースト期間が長く、レートが高い場合、バケットはオーバーフローし、そのバーストのフレームに対してポリシング アクションが実行されます。

バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドの *burst-byte* オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。トークンがバケットから削除される速度（平均速度）を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドの *rate-bps* オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。

次のタイプのポリシー マップが設定されると、図 37-4 のようなポリシングおよびマーキングのプロセスが実行されます。

- 物理ポートの非階層型ポリシー マップ。
- SVI に付加されたインターフェイス レベルの階層型ポリシー マップ。物理ポートは、このセカンダリ ポリシー マップに指定します。

図 37-4　物理ポートのポリシングおよびマーキング フローチャート



SVI のポリシング

（注）　SVI で個別ポリサーを持つ階層型ポリシー マップを設定する前に、SVI に属する物理ポート上で VLAN ベースの QoS をイネーブルにする必要があります。ポリシー マップが SVI に付加されていても、個別のポリサーは、階層型ポリシー マップのセカンダリ インターフェイス レベルで指定された物理ポート上のトラフィックにだけ影響を与えます。

階層ポリシー マップには 2 つのレベルがあります。1 つは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。もう 1 つはインターフェイス レベルで、インターフェイス レベルのポリシー マップに指定されていて、SVI に属する物理ポートのトラフィックに対して実行するアクションを指定します。

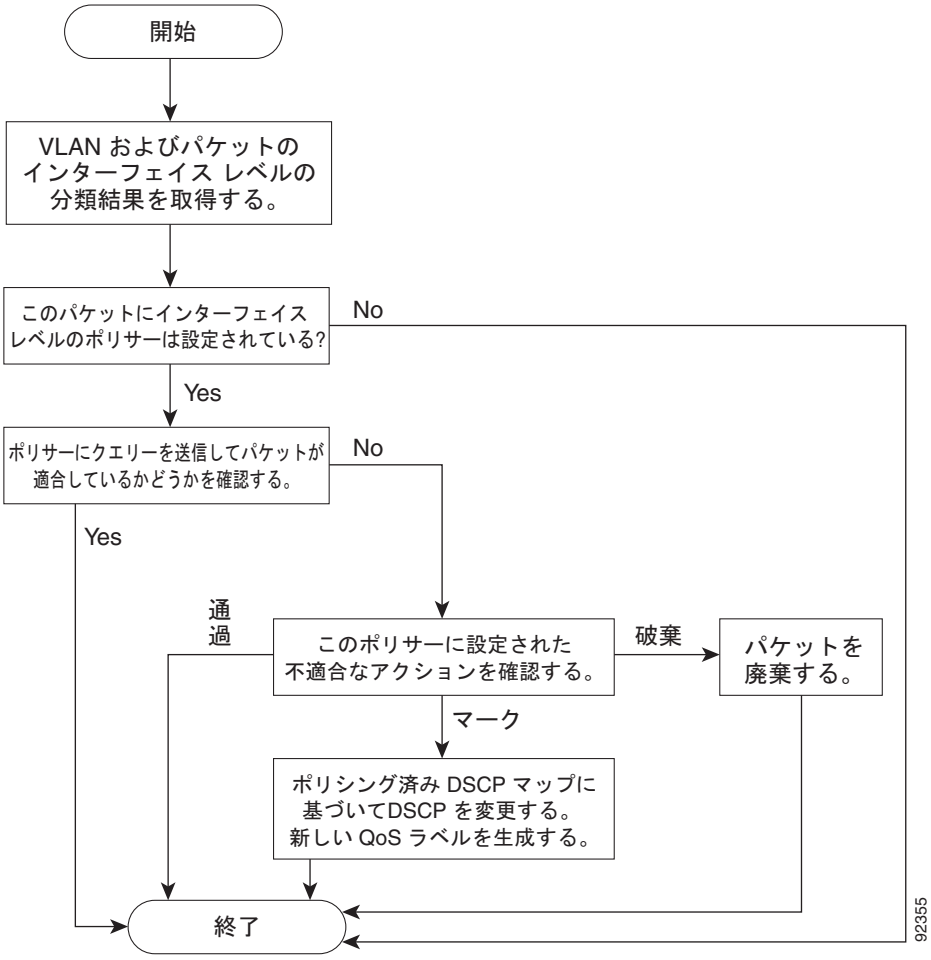
SVI にポリシングを設定する場合、次の 2 つのレベルの階層型ポリシー マップを作成および設定できます。

- VLAN レベル：クラス マップおよびポートの信頼状態を指定するクラスを設定することで、またはパケットに新規に DSCP や IP precedence 値を設定することでプライマリ レベルを作成します。VLAN レベルのポリシー マップは SVI の VLAN に対してだけ適用可能で、ポリサーはサポートしません。
- インターフェイス レベル：クラス マップおよび SVI の物理ポートに個別にポリサーを指定するクラスを設定することで、セカンダリ レベルを作成します。インターフェイス レベルのポリシー マップは個別のポリサーだけサポートし、集約ポリサーをサポートしません。VLAN レベルのポリシー マップで定義されたクラスごとに、異なるインターフェイス レベル ポリシー マップを設定できます。

階層型ポリシー マップの例については、「階層型ポリシー マップを使用した SVI のトラフィックの分類、ポリシング、およびマーキング」（P.37-66）を参照してください。

図 37-5 に、階層型ポリシー マップが SVI に付加されている場合のポリシングおよびマーキング プロセスを示します。

図 37-5　SVI のポリシングおよびマーキング フローチャート



マッピング テーブル

QoS を処理している間、すべてのトラフィック（非 IP トラフィックを含む）のプライオリティは、分類段階で取得された DSCP または CoS 値に基づく QoS ラベルで表されます。

- 分類中に、QoS は設定可能なマッピング テーブルを使用して、受信された CoS、DSCP、または IP precedence 値から、対応する DSCP または CoS 値を取得します。これらのマップには、CoS/DSCP マップや IP precedence/DSCP マップなどがあります。これらのマップを設定するには、**mls qos map cos-dscp** および **mls qos map ip-prec-dscp** グローバル コンフィギュレーション コマンドを使用します。

  DSCP 信頼状態で設定された入力ポートの DSCP 値が QoS ドメイン間で異なる場合は、2 つの QoS ドメイン間の境界にあるポートに、設定可能な DSCP/DSCP 変換マップを適用できます。このマップを設定するには、**mls qos map dscp-mutation** グローバル コンフィギュレーション コマンドを使用します。

- ポリシング中に、QoS は IP パケットまたは非 IP パケットに別の DSCP 値を割り当てることができます（パケットが不適合で、マークダウン値がポリサーによって指定されている場合）。この設定可能なマップは、ポリシング済み DSCP マップといいます。このマップを設定するには、**mls qos map policed-dscp** グローバル コンフィギュレーション コマンドを使用します。

- トラフィックがスケジューリング段階に達する前に、QoS は QoS ラベルに従って、入力および出力キューにパケットを格納します。QoS ラベルはパケット内の DSCP または CoS 値に基づいており、DSCP 入力および出力キューしきい値マップまたは CoS 入力および出力キューしきい値マップを使用してキューを選択します。入力キューか出力キューに加えて、QOS ラベルも WTD しきい値を識別します。これらのマップを設定するには、**mls qos srr-queue** {**input** | **output**} **dscp-map** および **mls qos srr-queue** {**input** | **output**} **cos-map** グローバル コンフィギュレーション コマンドを使用します。

CoS/DSCP、DSCP/CoS、および IP precedence/DSCP マップのデフォルト値は、使用しているネットワークに適する場合と適さない場合があります。

デフォルトの DSCP/DSCP 変換マップおよびデフォルトのポリシング設定 DSCP マップは、ヌル マップです。これらのマップでは、着信した DSCP 値が同じ DSCP 値にマッピングされます。DSCP/DSCP 変換マップは、特定のポートに適用できる唯一のマップです。その他のすべてのマップはスイッチ全体に適用されます。

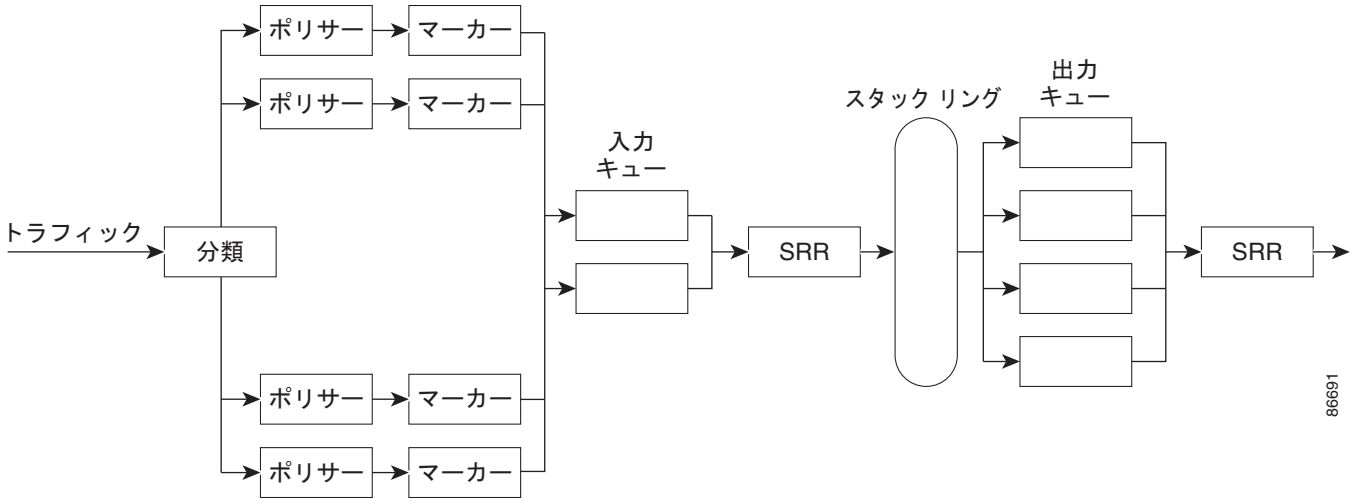
設定情報については、「DSCP マップの設定」（P.37-76）を参照してください。

DSCP および CoS 入力キューしきい値マップの詳細については、「入力キューのキューイングおよびスケジューリング」（P.37-16）を参照してください。DSCP および CoS 出力キューしきい値マップの詳細については、「出力キューのキューイングおよびスケジューリング」（P.37-18）を参照してください。

キューイングおよびスケジューリングの概要

スイッチは特定のポイントにキューを配置し、輻輳防止に役立てます（図 37-6 を参照）。

図 37-6　入力および出力キューの位置



すべてのポートの入力帯域幅の合計がスタックまたは内部リングの帯域幅を超えることがあるため、入力キューはパケットの分類、ポリシング、およびマーキングのあと、パケットがスイッチ ファブリックに転送される前の位置に配置されています。複数の入力ポートから 1 つの出力ポートに同時にパケットが送信されて、輻輳が発生することがあるため、出力キューはスタックまたは内部リングの後に配置されています。

WTD

入力キューと出力キューは両方とも、Weighted Tail Drop（WTD）と呼ばれるテールドロップ輻輳回避メカニズムの拡張バージョンを使用します。WTD はキュー長を管理したり、トラフィック分類ごとに異なるドロップ優先順位を設定したりするために実装されています。

フレームが特定のキューに送信されると、WTD はフレームの割り当て QoS ラベルを使用して、それぞれ異なるしきい値を適用します。この QoS ラベルのしきい値を超えると（宛先キューの空きスペースがフレーム サイズより小さくなると）、フレームはドロップされます。

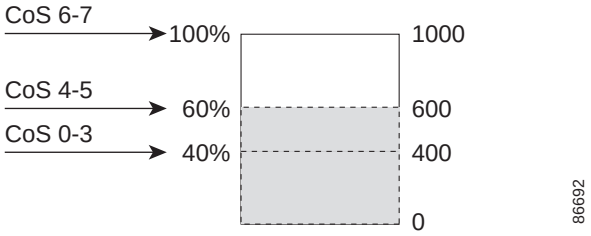
各キューには 3 つのしきい値があります。3 つのしきい値のうちどれがフレームに適用されるかは、QOS ラベルによって決まります。3 つのしきい値のうち 2 つは設定可能（明示的）ですが、1 つは設定可能ではありません（暗黙）。

図 37-7 に、サイズが 1000 フレームであるキューでの WTD の動作例を示します。ドロップ割合は次のように設定されています。40%（400 フレーム）、60%（600 フレーム）、および 100%（1000 フレーム）です。これらのパーセンテージは、40% しきい値の場合は最大 400 フレーム、60% しきい値の場合は最大 600 フレーム、100% しきい値の場合は最大 1000 フレームをキューイングできるという意味です。

この例では、CoS 値 6 および 7 は他の CoS 値よりも重要度が高く、100% ドロップしきい値に割り当てられます（キューフル ステート）。CoS 値 4 および 5 は 60% しきい値に、CoS 値 0 ～ 3 は 40% しきい値に割り当てられます。

600 個のフレームが格納されているキューに、新しいフレームが着信したとします。このフレームの CoS 値は 4 および 5 で、60% のしきい値が適用されます。このフレームがキューに追加されると、しきい値を超過するため、フレームはドロップされます。

図 37-7　WTD およびキューの動作



詳細については、「入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定」（P.37-83）、「出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定」（P.37-87）、および「出力キューおよびしきい値 ID への DSCP または CoS 値のマッピング」（P.37-89）を参照してください。

SRR のシェーピングおよび共有

入力キューおよび出力キューはいずれも SRR で処理され、SRR によってパケットの送信レートが制御されます。入力キューでは、SRR によってパケットがスタックまたは内部リングに送信されます。出力キューでは、SRR によってパケットが出力ポートに送信されます。

出力キューでは、SRR を共有またはシェーピング用に設定できます。ただし、入力キューでは共有がデフォルトモードであり、これ以外のモードはサポートされていません。

シェーピング モードでは、出力キューは帯域幅のパーセントとして保証され、この量にレート制限されます。リンクがアイドルの場合でも、シェーピングされたトラフィックは割り当てられた帯域幅を越えて使用できません。シェーピングを使用すると、時間あたりのトラフィック フローがより均一になり、バースト トラフィックの最高時と最低時を削減します。シェーピングの場合は、各重みの絶対値を使用して、キューに使用可能な帯域幅が計算されます。

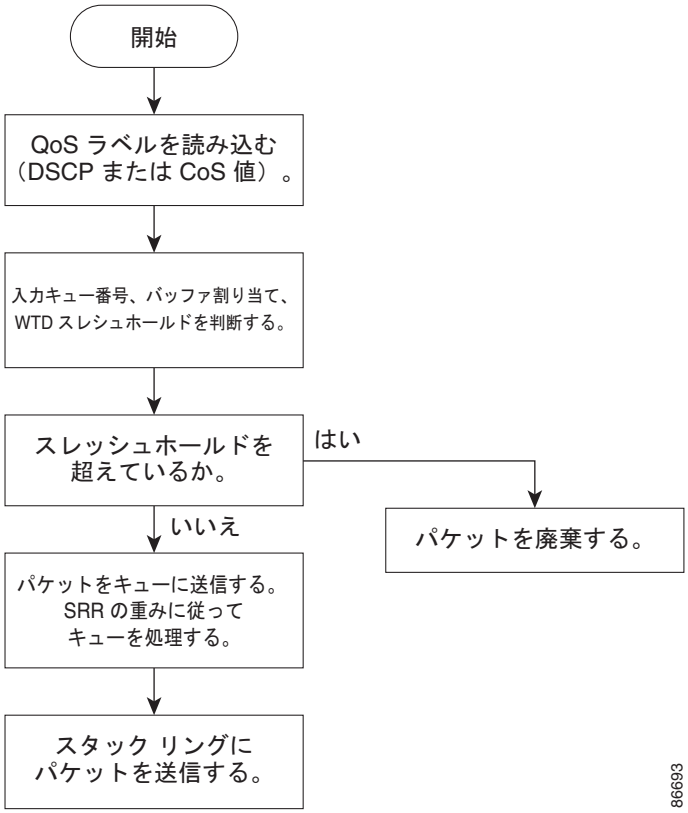
共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、特定のキューが空であり、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有できます。共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関係ありません。シェーピングと共有はインターフェイスごとに設定します。各インターフェイスは固有に設定できます。

詳細については、「入力キュー間の帯域幅の割り当て」（P.37-85）、「出力キューの SRR シェーピング重みの設定」（P.37-91）、および「出力キューでの SRR 共有重みの設定」（P.37-92）を参照してください。

入力キューのキューイングおよびスケジューリング

図 37-8 に、入力ポートのキューイングおよびスケジューリング フローチャートを示します。

図 37-8　入力ポートのキューイングおよびスケジューリング フローチャート



（注）　共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

スイッチは、共有モードの SRR によってだけ処理される、設定可能な入力キューを 2 つサポートしています。表 37-1 にこれらのキューの説明を示します。

表 37-1　入力キューのタイプ

キュー タイプ[1]	機能
標準	標準プライオリティと見なされるユーザ トラフィック。各フローを区別するために、3 つの異なるしきい値を設定できます。**mls qos srr-queue input threshold**、**mls qos srr-queue input dscp-map**、および **mls qos srr-queue input cos-map** グローバル コンフィギュレーション コマンドを使用できます。
緊急	差別化サービス緊急転送または音声トラフィックなどのハイプライオリティ ユーザ トラフィック。このトラフィックに必要な帯域幅は、**mls qos srr-queue input priority-queue** グローバル コンフィギュレーション コマンドを使用して、合計トラフィックまたは合計スタック トラフィックの割合として設定できます。緊急キューには帯域幅が保証されています。

1. スイッチでは、設定不可能なトラフィック用キューが 2 つ使用されます。これらのキューは、ネットワークおよびスタックを適切に動作させるために重要です。

キューおよびしきい値にスイッチを通過する各パケットを割り当てます。特に、入力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。**mls qos srr-queue input dscp-map queue** *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id dscp1...dscp8*} または **mls qos srr-queue input cos-map queue** *queue-id* {*cos1...cos8* | **threshold** *threshold-id cos1...cos8*} グローバル コンフィギュレーション コマンドを使用します。DSCP 入力キューしきい値マップおよび CoS 入力キューしきい値マップを表示するには、**show mls qos maps** 特権 EXEC コマンドを使用します。

WTD しきい値

キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。各キューには 3 つのドロップしきい値があります。そのうちの 2 つは設定可能（*明示的*）な WTD しきい値で、もう 1 つはキューフル ステートに設定済みの設定不可能（*暗示的*）なしきい値です。入力キューに 2 つの明示的 WTD しきい値の割合（しきい値 ID 1 および ID 2 用）を割り当てるには、**mls qos srr-queue input threshold** *queue-id threshold-percentage1 threshold-percentage2* グローバル コンフィギュレーション コマンド を使用します。各しきい値は、キューに割り当てられたバッファの合計値に対する割合です。しきい値 ID 3 のドロップしきい値は、キューフル ステートに設定済みで、変更できません。WTD の仕組みの詳細については、「WTD」（P.37-14）を参照してください。

バッファおよび帯域幅の割り当て

2 つのキュー間の入力バッファを分割する比率を定義する（スペース量を割り当てる）には、**mls qos srr-queue input buffers** *percentage1 percentage2* グローバル コンフィギュレーション コマンドを使用します。バッファ割り当てと帯域幅割り当てを組み合わせることにより、パケットがドロップされる前にバッファに格納して送信できるデータ量が制御されます。帯域幅を割合として割り当てるには、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドを使用します。重みの比率は、SRR スケジューラがパケットを各キューから送り出す頻度の比率です。

プライオリティ キューイング

特定の入力キューをプライオリティ キューとして設定するには、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドを使用します。プライオリティ キューはスタックまたは内部リングの負荷にかかわらず帯域幅の一部が保証されているため、確実な配信を必要とするトラフィック（音声など）に使用する必要があります。

SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に、SRR は **mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。

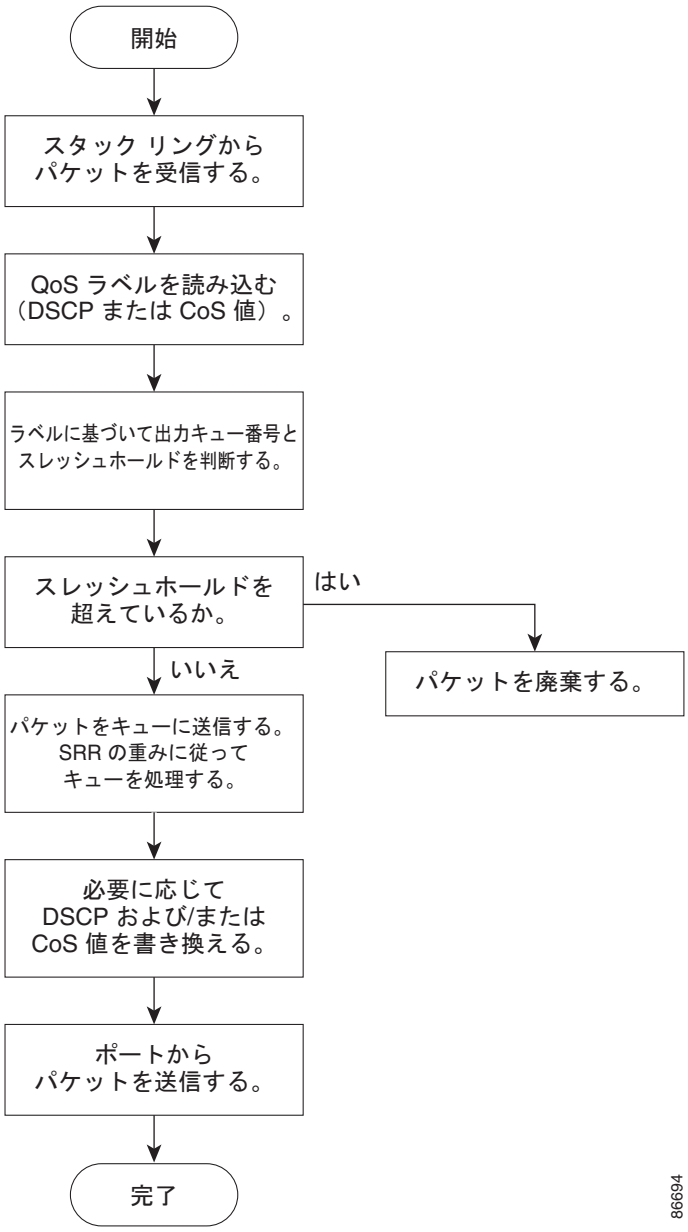
ここに記載されたコマンドを組み合わせると、特定の DSCPs または CoSs を持つパケットを特定のキューに格納したり、大きいキュー サイズを割り当てたり、キューの処理頻度を増やしたり、プライオリティが低いパケットがドロップされるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定することができます。設定情報については、「入力キューの特性の設定」（P.37-82）を参照してください。

出力キューのキューイングおよびスケジューリング

図 37-9 に、出力ポートのキューイングおよびスケジューリング フローチャートを示します。

（注）　緊急キューがイネーブルの場合、SRR によって空になるまで処理されてから、他の 3 つのキューが処理されます。

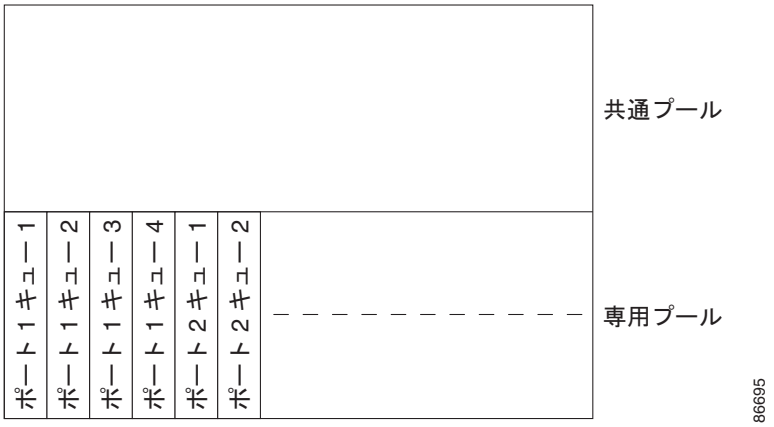
図 37-9　出力ポートのキューイングおよびスケジューリング フローチャート



各ポートは 4 つの出力キューをサポートし、そのうちの 1 つ（キュー 1）を出力緊急キューにすることができます。これらのキューはキューセットに割り当てられます。スイッチから送信されるすべてのトラフィックは、パケットに割り当てられた QoS ラベルに基づいて、これらの 4 つのキューのいずれかを通過し、しきい値の影響を受けます。

図 37-10 に出力キューセットのバッファを示します。バッファ スペースは共通プールと専用プールからなります。スイッチはバッファ割り当て方式を使用して、出力キューごとに最小バッファ サイズを確保します。これにより、いずれかのキューまたはポートがすべてのバッファを消費して、その他のキューのバッファが不足することがなくなり、要求元のキューにバッファ スペースを割り当てるかどうかが制御されます。スイッチは、ターゲット キューが予約量を超えるバッファを消費していないかどうか（アンダーリミット）、その最大バッファをすべて消費したかどうか（オーバーリミット）、共通のプールが空（空きバッファがない）か空でない（空きバッファ）かを判断します。キューがオーバーリミットでない場合は、スイッチは予約済みプールまたは共通のプール（空でない場合）からバッファ スペースを割り当てることができます。共通のプールに空きバッファがない場合や、キューがオーバーリミットの場合、スイッチはフレームをドロップします。

図 37-10　　出力キューのバッファ割り当て



バッファおよびメモリの割り当て

バッファのアベイラビリティの保証、ドロップしきい値の設定、およびキューセットの最大メモリ割り当ての設定を行うには、**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* グローバル コンフィギュレーション コマンドを使用します。各しきい値はキューに割り当てられたメモリの割合です。パーセンテージを指定するには、**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4* グローバル コンフィギュレーション コマンドを使用します。割り当てられたすべてのバッファの合計が専用プールになります。残りのバッファは共通プールの一部になります。

バッファ割り当てを行うと、ハイプライオリティ トラフィックを確実にバッファに格納できます。たとえば、バッファ スペースが 400 の場合、バッファ スペースの 70% をキュー 1 に割り当てて、10% をキュー 2 ～ 4 に割り当てることができます。キュー 1 には 280 のバッファが割り当てられ、キュー 2 ～ 4 にはそれぞれ 40 バッファが割り当てられます。

割り当てられたバッファをキューセット内の特定のキュー用に確保するよう保証できます。たとえば、キュー用として 100 バッファがある場合、50%（50 バッファ）を確保できます。残りの 50 バッファは共通プールに戻されます。また、最大しきい値を設定することにより、一杯になったキューが確保量を超えるバッファを取得できるようにすることもできます。共通プールが空でない場合、必要なバッファを共通プールから割り当てることができます。

WTD しきい値

スイッチを通過する各パケットをキューおよびしきい値に割り当てることができます。特に、出力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。**mls qos srr-queue output dscp-map queue** *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id* **dscp1...dscp8**} または *mls qos srr-queue output cos-map queue queue-id* {**cos1...cos8** | *threshold* threshold-id cos1...cos8} グローバル コンフィギュレーション コマンドを使用します。DSCP 出力キューしきい値マップおよび CoS 出力キューしきい値マップを表示するには、**show mls qos maps** 特権 EXEC コマンドを使用します。

キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。各キューには 3 つのドロップしきい値があります。そのうちの 2 つは設定可能（*明示的*）な WTD しきい値で、もう 1 つはキューフル ステートに設定済みの設定不可能（*暗示的*）なしきい値です。しきい値 ID 1 および ID 2 用の 2 つの WTD しきい値割合を割り当てます。しきい値 ID 3 のドロップしきい値は、キューフル ステートに設定済みで、変更できません。ポートをキューセットにマッピングするには、**queue-set** *qset-id* インターフェイス コンフィギュレーション コマンドを使用します。WTD しきい値の割合を変更するには、キューセット設定を変更します。WTD の仕組みの詳細については、「WTD」（P.37-14）を参照してください。

シェーピング モードまたは共有モード

SRR は、シェーピング モードまたは共有モードで各キューセットを処理します。ポートをキューセットにマッピングするには、queue-set qset-id インターフェイス コンフィギュレーション コマンドを使用します。ポートに共有重みまたはシェーピング重みを割り当てるには、**srr-queue bandwidth share** *weight1 weight2 weight3 weight4* または **srr-queue bandwidth shape** *weight1 weight2 weight3 weight4* インターフェイス コンフィギュレーション コマンドを使用します。シェーピングと共有の違いについては、「SRR のシェーピングおよび共有」（P.37-15）を参照してください。

バッファ割り当てと SRR 重み比率を組み合わせることにより、パケットがドロップされる前にバッファに格納して送信できるデータ量が制御されます。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

緊急キューがイネーブルになっていない限り、4 つのキューすべてが SRR に参加します。この場合、最初の帯域幅の重みは無視され、比率計算には使用されません。緊急キューはプライオリティ キューであり、他のキューのサービスが提供される前に空になるまでサービスを提供します。緊急キューをイネーブルにするには、**priority-queue out** インターフェイス コンフィギュレーション コマンドを使用します。

ここに記載されたコマンドを組み合わせると、特定の DSCPs または CoSs を持つパケットを特定のキューに格納したり、大きいキュー サイズを割り当てたり、キューの処理頻度を増やしたり、プライオリティが低いパケットがドロップされるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定することができます。設定情報については、「出力キューの特性の設定」（P.37-86）を参照してください。

（注）出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合のみ、設定を変更してください。

パケットの変更

QoS を設定するには、パケットの分類、ポリシング、キューイングを行います。このプロセス中に、次のようにパケットが変更されることがあります。

- IP パケットおよび非 IP パケットの分類では、受信パケットの DSCP または CoS に基づいて、パケットに QoS ラベルが割り当てられます。ただし、この段階ではパケットは変更されません。割り当てられた DSCP または CoS 値の指定だけがパケットとともに伝達されます。これは、QoS の分類および転送検索が並行して発生するためです。パケットを元の DSCP のまま CPU に転送し、CPU でソフトウェアによる再処理を行うことができます。
- ポリシング中は、IP および非 IP パケットに別の DSCP を割り当てることができます（これらのパケットが不適合で、ポリサーが DSCP のマークダウンを指定している場合）。この場合も、パケット内の DSCP は変更されず、マークダウン値の指定がパケットとともに伝達されます。IP パケットの場合は、この後の段階でパケットが変更されます。非 IP パケットの場合は、DSCP が CoS に変換され、キューイングおよびスケジューリングの決定に使用されます。
- フレームに割り当てられた QoS ラベル、および選択された変換マップに応じて、フレームの DSCP および CoS 値が書き換えられます。変換マップが設定されておらず、着信フレームの DSCP を信頼するようにポートが設定されている場合、フレーム内の DSCP 値は変更されないで、DSCP/CoS マップに従って CoS が書き換えられます。着信フレームの CoS を信頼するようにポートが設定されていて、着信フレームが IP パケットの場合、フレーム内の CoS 値は変更されませんが、DSCP は CoS/DSCP マップに従って変更されることがあります。

  入力変換が行われると、選択された新しい DSCP 値に応じて DSCP が書き換えられます。ポリシー マップの設定アクションによっても、DSCP が書き換えられます。

自動 QoS の設定

自動 QoS 機能を使用して、QoS 機能の配置を容易にできます。自動 QoS は、ネットワーク設計を判定し、QoS コンフィギュレーションをイネーブルにすることで、異なるトラフィック フローに対してプライオリティを指定できます。この機能では、デフォルトの QoS 動作（ディセーブル）を使用する代わりに、入力キューと出力キューが使用されます。スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供し、単一キューからパケットを送信します。

自動 QoS をイネーブルにすると、トラフィック タイプおよび入力パケット ラベルに基づいてトラフィックを自動的に分類します。スイッチは分類した結果を使用して適切な出力キューを選択します。

Cisco IOS Release 12.2(52)SE 以降のリリースでは、**sdm prefer dual ipv4-and-ipv6** グローバル コンフィギュレーション コマンドによってデュアル IPv4/IPv6 SDM テンプレートが設定されている場合、自動 QoS は IPv4 および IPv6 のトラフィックがサポートされます。

自動 QoS コマンドを使用して、次のシスコ デバイスに接続されているポートを特定します。

- Cisco IP Phone
- Cisco SoftPhone アプリケーションが動作するデバイス
- Cisco TelePresence
- Cisco IP カメラ

また、アップリンクを介して信頼のおけるトラフィックを受信するポートを指定します。自動 QoS は次の機能を実行します。

- 条件付き信頼を備えたインターフェイスによる自動 QoS デバイスの有無の検出
- QoS 分類の設定
- 出力キューの設定

ここでは、次の設定情報について説明します。

- Cisco IP Phone の有無を検知します。
- QoS 分類の設定
- 出力キューの設定

ここでは、次の設定情報について説明します。

- 「生成される自動 QoS 設定」（P.37-22）
- 「コンフィギュレーションにおける自動 QoS の影響」（P.37-32）
- 「自動 QoS 設定時の注意事項」（P.37-32）
- 「自動 QoS のイネーブル化」（P.37-33）
- 「自動 QoS コマンドのトラブルシューティング」（P.37-34）

生成される自動 QoS 設定

デフォルトでは、自動 QoS はすべてのポートでディセーブルです。パケットは変更されず、パケットの CoS、DSCP、および IP precedence の各値は変わりません。

インターフェイスの最初のポートで自動 QoS 機能をイネーブルにすると、次のアクションが実行されます。

- 入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力/出力キューの設定が行われます。
- QoS がグローバルにイネーブルになり（**mls qos** グローバル コンフィギュレーション コマンド）、他のグローバル コンフィギュレーション コマンドが自動生成されます。（表 37-5 を参照）。
- スイッチは信頼境界機能をイネーブルにし、Cisco Discovery Protocol（CDP）を使用して、サポートされているデバイスの存在を検出します。
- スイッチはまた、ポリシングを使用してパケットがプロファイル内かプロファイル外かを判断し、パケットに対するアクションを指定します。

VOIP デバイスの特質

- **auto qos voip cisco-phone** コマンドを Cisco IP Phone が接続されたネットワーク エッジにあるポートに入力すると、スイッチは信頼境界機能をイネーブルにします。パケットに 24、26、または 46 の DSCP 値がない場合、またはパケットがアウト オブ プロファイルの場合は、スイッチで DSCP 値が 0 に変更されます。Cisco IP Phone が存在しない場合、入力分類はパケットの QoS ラベルを信頼しないよう設定されます。ポリシングがポリシーマップ分類と一致したトラフィックに適用された後で、スイッチが信頼境界の機能をイネーブルにします。
- **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを、Cisco SoftPhone を稼動するデバイスに接続されたネットワークのエッジのポートに入力すると、スイッチはポリシングを使用して、パケットがイン プロファイルかアウト オブ プロファイルかを判断し、パケット上の処理を指定します。パケットに 24、26、または 46 の DSCP 値がない場合、またはパケットがアウト オブ プロファイルの場合は、スイッチで DSCP 値が 0 に変更されます。
- ネットワーク内部に接続されたポート上で、**auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力した場合、スイッチは、入力パケットでルーティングされないポートの CoS 値、またはルーテッド ポートの DSCP 値を信頼します（トラフィックが他のエッジ デバイスですでに分類されていることが前提条件になります）。

スイッチは、表 37-3 および表 37-4 の設定値に従ってポートの入力キューと出力キューを設定します。

表 37-2　トラフィック タイプ、パケット ラベル、キュー

	VoIP [1] データ トラフィック	VoIP コントロール トラフィック	ルーティング プロトコル トラフィック	STP BPDU トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP	46	24、26	48	56	34	–	
CoS	5	3	6	7	3	–	
CoS/入力キューマップ	4、5（キュー 2）					0、1、2、3、6、7（キュー 1）	
CoS/出力キューマップ	4、5（キュー 1）	2、3、6、7（キュー 2）			0（キュー 3）	2（キュー 3）	0、1（キュー 4）

1. VoIP = Voice over IP

表 37-3　入力キューに対する自動 QoS の設定

入力キュー	キュー番号	CoS からキューへのマッピング	キューの重み（帯域幅）	キュー（バッファ）サイズ
SRR 共有	1	0、1、2、3、6、7	70%	90%
プライオリティ	2	4、5	30%	10%

表 37-4　出力キューに対する自動 QoS の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キューの重み（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

信頼境界機能については、39-42 ページの「Configuring a Trusted Boundary to Ensure Port Security」の項を参照してください。

auto qos voip cisco-phone、**auto qos voip cisco-softphone**、または **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを使用して自動 QoS をイネーブルにすると、スイッチはトラフィック タイプと入力パケット ラベルに基づいて自動的に QoS 設定を生成し、表 37-5 に示すコマンドをポートに適用します。

ビデオ、信頼、および分類用の拡張自動 QoS

CiscoIOS Release 12.2(55)SE では、自動 QoS がビデオをサポートするように拡張されています。Cisco TelePresence システムと Cisco IP カメラからのトラフィックを分類および信頼する自動設定が生成されます。

スイッチ ポートで **auto qos** {**video** | **classify** | **trust**} 拡張コマンドを設定すると、次の動作が実行されます。

- Cisco IOS Release 12.2(55)SE より前のインターフェイスで設定した **auto qos voip** 生成コマンドが、拡張コマンドに移行します。
- 拡張コマンドの移行とともに、グローバル値が変更されます。実行コンフィギュレーションに適用される生成コマンドの一覧については、表 37-5 を参照してください。

自動 QoS 設定の移行

レガシー自動 QoS から拡張自動 QoS への自動 QoS 設定の移行は、次のように実行されます。

- スイッチが 12.2(55)SE イメージで起動されます。QoS はディセーブルです。

  インターフェイス上のビデオおよび音声の信頼設定によって、自動的に拡張自動 QoS コマンドが生成されます。
- スイッチで QoS がイネーブルになり、次のガイドラインに従って処理が行われます。
  - 音声デバイス上に条件付き信頼用のインターフェイスを設定する場合、レガシー自動 QoS VoIP 設定のみが生成されます。
  - ビデオ デバイス上に条件付き信頼用のインターフェイスを設定する場合、拡張自動 QoS 設定が生成されます。
  - 新しいインターフェイスの自動 QoS コマンドに基づいて、分類または条件付き信頼を備えたインターフェイスを設定する場合、拡張自動 QoS 設定が生成されます。
- 自動 QoS の移行は、**auto qos srnd4** グローバル コンフィギュレーション コマンドがイネーブルになり、新しいデバイスが接続された後に実行されます。

（注）レガシー自動 QoS を使用して設定されているインターフェイスを、拡張自動 QoS に移行する場合、音声コマンドと設定が、新しいグローバル QoS コマンドに合せて更新されます。

拡張された自動 QoS からレガシー自動 QoS への自動 QoS の移行は、既存のすべての自動 QoS 設定をインターフェイスからディセーブルした場合のみ実行できます。

グローバル自動 QoS 設定

表 37-5　生成される自動 QoS 設定

説明	自動的に生成されるコマンド {voip}	自動的に生成される拡張コマンド {Video|Trust|Classify}
スイッチは標準 QoS を自動的にイネーブルにし、CoS/DSCP マップ（着信パケット内の CoS 値の DSCP 値へのマッピング）を設定します。	Switch(config)# **mls qos** Switch(config)# **mls qos map cos-dscp 0 8 16 26 32 46 48 56**	Switch(config)# **mls qos** Switch(config)# **mls qos map cos-dscp 0 8 16 24 32 46 48 56**
スイッチが、自動的に CoS 値を入力キューおよびしきい値 ID にマッピングします。	Switch(config)# **no mls qos srr-queue input cos-map** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 2 1** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 3 0** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 1 2** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 3 3 5**	Switch(config)# **no mls qos srr-queue input cos-map** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 2 3** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 3 6 7** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 1 4**
スイッチが、自動的に CoS 値を出力キューおよびしきい値 ID にマッピングします。	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 2 4** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 2 1** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 0**	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 4 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 1 2** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 2 3** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 0** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 1**

表 37-5　生成される自動 QoS 設定（続き）

説明	自動的に生成されるコマンド {voip}	自動的に生成される拡張コマンド {Video|Trust|Classify}
スイッチが、自動的に DSCP 値を入力キューおよびしきい値 ID にマッピングします。	Switch(config)# **no mls qos srr-queue input dscp-map** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 32** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47**	Switch(config)# **no mls qos srr-queue input dscp-map** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 2 24** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41 42 43 44 45** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 46 47**

表 37-5　生成される自動 QoS 設定（続き）

説明	自動的に生成されるコマンド {voip}	自動的に生成される拡張コマンド {Video|Trust|Classify}
スイッチが、自動的に DSCP 値を出力キューおよびしきい値 ID にマッピングします。	Switch(config)# **no mls qos srr-queue output dscp-map** Switch(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7**	Switch(config)# **no mls qos srr-queue output dscp-map** Switch(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41 42 43 44 45 46 47** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35 36 37 38 39** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 2 24** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5 6 7** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14**

表 37-5　生成される自動 QoS 設定（続き）

説明	自動的に生成されるコマンド {voip}	自動的に生成される拡張コマンド {Video|Trust|Classify}
スイッチが自動的に入力キューを設定します。キュー 2 がプライオリティ キューでキュー 1 が共有モードです。また、スイッチは、入力キューの帯域幅とバッファ サイズも設定します。	Switch(config)# **no mls qos srr-queue input priority-queue 1** Switch(config)# **no mls qos srr-queue input priority-queue 2** Switch(config)# **mls qos srr-queue input bandwidth 90 10** Switch(config)# **mls qos srr-queue input threshold 1 8 16** Switch(config)# **mls qos srr-queue input threshold 2 34 66** Switch(config)# **mls qos srr-queue input buffers 67 33**	Switch(config)# **no mls qos srr-queue input priority-queue 1** Switch(config)# **no mls qos srr-queue input priority-queue 2** Switch(config)# **mls qos srr-queue input bandwidth 70 30** Switch(config)# **mls qos srr-queue input threshold 1 80 90** Switch(config)# **mls qos srr-queue input priority-queue 2 bandwidth 30**
スイッチは出力キューのバッファ サイズを自動的に設定します。ポートにマッピングされた出力キューの帯域幅と SRR モード（シェーピングまたは共有）を設定します。	Switch(config)# **mls qos queue-set output 1 threshold 1 138 138 92 138** Switch(config)# **mls qos queue-set output 1 threshold 2 138 138 92 400** Switch(config)# **mls qos queue-set output 1 threshold 3 36 77 100 318** Switch(config)# **mls qos queue-set output 1 threshold 4 20 50 67 400** Switch(config)# **mls qos queue-set output 2 threshold 1 149 149 100 149** Switch(config)# **mls qos queue-set output 2 threshold 2 118 118 100 235** Switch(config)# **mls qos queue-set output 2 threshold 3 41 68 100 272** Switch(config)# **mls qos queue-set output 2 threshold 4 42 72 100 242** Switch(config)# **mls qos queue-set output 1 buffers 10 10 26 54** Switch(config)# **mls qos queue-set output 2 buffers 16 6 17 61** Switch(config-if)# **priority-que out** Switch(config-if)# **srr-queue bandwidth share 10 10 60 20**	Switch(config)# **mls qos queue-set output 1 threshold 2 100 100 50 200** Switch(config)# **mls qos queue-set output 1 threshold 2 125 125 100 400** Switch(config)# **mls qos queue-set output 1 threshold 3 100 100 100 400** Switch(config)# **mls qos queue-set output 1 threshold 4 60 150 50 200** Switch(config)# **mls qos queue-set output 1 buffers 15 25 40 20**

自動 QoS によって生成される VoIP デバイス用の設定

auto qos voip cisco-phone コマンドを入力すると、スイッチが自動的に信頼境界機能をイネーブルにし、CDP を使用して Cisco IP Phone の有無を検出します。

```
Switch(config-if)# mls qos trust device cisco-phone
```

auto qos voip cisco-softphone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。

```
Switch(config)# mls qos map policed-dscp 24 26 46 to 0
Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust
Switch(config-cmap)# d match ip dscp ef
Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust
Switch(config-cmap)# match ip dscp cs3 af31
Switch(config)# policy-map AutoQoS-Police-SoftPhone
Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit
```

```
Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
```

クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ（*AutoQoS-Police-SoftPhone*）を、Cisco SoftPhone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します。

```
Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone
```

auto qos voip cisco-phone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。

```
Switch(config-if)# mls qos trust device cisco-phone
```

auto qos voip cisco-softphone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。

```
Switch(config)# mls qos map policed-dscp 24 26 46 to 0
Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust
Switch(config-cmap)# match ip dscp cs3 af31
Switch(config)# policy-map AutoQoS-Police-CiscoPhone
Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
```

クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ（*AutoQoS-Police-SoftPhone*）を、Cisco SoftPhone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します。

```
Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone
```

自動 QoS によって生成される拡張ビデオ、信頼、およびデバイスの分類用の設定

次の拡張自動 QoS コマンドを入力すると、スイッチは、CoS/DSCP マップ（着信パケット内の CoS 値の DSCP 値へのマッピング）を自動的に設定します。

- **auto qos video cts**
- **auto qos video ip-camera**
- **auto qos trust**
- **auto qos trust cos**
- **auto qos trust dscp**

```
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
```

（注）　クラス マップやポリシー マップは設定されません。

auto qos classify コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。

```
Switch(config)# mls qos map policed-dscp  0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Switch(config)# policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
Switch(config-pmap)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-CLASSIFY-POLICY
```

auto qos classify police コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。

```
Switch(config)# mls qos map policed-dscp  0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Switch(config)# policy-map AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
Switch(config-pmap)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap-c)# police 5000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap-c)# police 10000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
```

```
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
```

auto qos voip cisco-phone コマンドの拡張設定は次のとおりです。

```
Switch(config)# mls qos map policed-dscp  0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
Switch(config)# policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
```

auto qos voip cisco-softphone コマンドの拡張設定は次のとおりです。

```
Switch(config)# mls qos map policed-dscp  0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER

Switch(config)# policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap-c)# police 5000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
```

```
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap-c)# police 10000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-SOFTPHONE-POLICY
```

コンフィギュレーションにおける自動 QoS の影響

自動 QoS がイネーブルの場合、**auto qos** インターフェイス コンフィギュレーション コマンドおよび生成されたグローバル設定が実行コンフィギュレーションに追加されます。

スイッチは、自動 QoS が生成したコマンドを、CLI から入力したように適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。生成コマンドが適用されなかった場合、以前の実行コンフィギュレーションが復元されます。

自動 QoS 設定時の注意事項

自動 QoS を設定する前に、次の事項を確認してください。

- 自動 QoS をイネーブルにしたあと、名前に *AutoQoS* を含むポリシーマップまたは集約ポリサーを変更しないでください。ポリシー マップまたは集約ポリサーを変更する必要がある場合、これらをコピーしてから、コピーしたポリシー マップまたは集約ポリサーを変更してください。生成したポリシー マップではなくこの新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除し、新しいポリシー マップをインターフェイスに適用します。
- 自動 QoS のデフォルトを利用する場合、他の QoS コマンドを設定する前に、自動 QoS をイネーブルにする必要があります。必要に応じて QoS 設定を微調整できますが、自動 QoS が完了した後にだけ調整することを推奨します。詳細については、8 ページの「Effects of Auto-QoS on the Configuration」を参照してください。
- 自動 QoS は、スタティック アクセス、ダイナミック アクセス、音声 VLAN アクセス、およびトランク ポートでイネーブルにできます。
- デフォルトでは、CDP 機能はすべてのポート上でイネーブルです。自動 QoS が適切に動作するために、CDP をディセーブルにしないでください。

自動 QoS VoIP に関する考慮事項

- 非ルーテッドおよびルーテッド ポート上で Cisco IP Phone が接続されている VoIP のスイッチを、自動 QoS が設定します。また、自動 QoS は Cisco SoftPhone アプリケーションを稼動するデバイスの VoIP 用にスイッチを設定します。

（注）　Cisco SoftPhone を稼動するデバイスが非ルーテッド ポートまたはルーテッド ポートに接続されている場合、スイッチはポート単位で Cisco SoftPhone アプリケーション 1 つだけをサポートします。

- ルーテッド ポートで Cisco IP Phone の自動 QoS をイネーブルにする場合、スタティック IP アドレスを IP Phone に割り当てる必要があります。
- このリリースは、Cisco IP SoftPhone Version 1.3(3) 以降だけをサポートします。
- 接続される装置は Cisco CallManager バージョン 4 以降を使用する必要があります。

拡張された自動 QoS に関する考慮事項

- **auto qos srnd4** グローバル コンフィギュレーション コマンドは、拡張された自動 QoS 設定の結果として生成されます。
- スイッチでレガシー **auto qos voip** コマンドが実行され、**mls qos** コマンドがディセーブルの場合、拡張された自動 QoS 設定が生成されます。そうでない場合、レガシーの自動 QoS コマンドが実行されます。

自動 QoS のイネーブル化

QoS パフォーマンスを最適にするには、ネットワーク内部のデバイスすべてで自動 QoS をイネーブルにします。

QoS ドメイン内で自動 QoS デバイスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	ビデオ デバイスに接続されたポートまたはネットワーク内の別の信頼できるスイッチまたはルータに接続されたアップリンク ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**auto qos voip** {**cisco-phone** | **cisco-softphone** | **trust**} または	自動 QoS をイネーブルにします。 • **cisco-phone**：ポートが Cisco IP Phone に接続されている場合、着信パケットの QoS ラベルは電話機が検出されたときだけ信頼されます。 • **cisco-softphone**：ポートが Cisco SoftPhone 機能を実行するデバイスに接続されています。 • **trust**：アップリンク ポートが信頼性のあるスイッチまたはルータに接続されていて、入力パケットの VoIP トラフィック分類が信頼されています。

	コマンド	目的
	auto qos video {**cts** | **ip-camera**} または	ビデオ デバイス用の自動 QoS をイネーブルにします。 • **cts** : Cisco TelePresence システムに接続されているポート • **ip-camera** : IP カメラに接続されているポート 着信パケットの QoS ラベルが信頼されるのは、システムが検知される場合に限ります。
	auto qos classify [**police**] または	分類用の自動 QoS をイネーブルにします。 • **police** : QoS ポリシー マップを定義し、それらをポートに適用することでポリシングを設定します（ポートベースの QoS）。
	auto qos trust {**cos** | **dscp**}	信頼できるインターフェイス用の自動 QoS をイネーブルにします。 • **cos** : サービス クラス • **dscp** : 差別化サービス コード ポイント
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** *interface-id*	信頼性のあるスイッチまたはルータに接続していると認識されるスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**auto qos trust**	ポート上で自動 QoS をイネーブルにし、そのポートが信頼性のあるルータまたはスイッチに接続されるように指定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show auto qos interface** *interface-id*	設定を確認します。 このコマンドは、自動 QoS がイネーブルであるインターフェイス上の自動 QoS コマンドを表示します。自動 QoS 設定およびユーザの変更を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

自動 QoS コマンドのトラブルシューティング

自動 QoS のイネーブルまたはディセーブル時に自動的に生成された QoS コマンドを表示するには、自動 QoS をイネーブルにする*前に*、**debug auto qos** 特権 EXEC コマンドを入力します。詳細については、このリリースに対応するコマンド リファレンスにある **debug autoqos** コマンドを参照してください。

ポート上で自動 QoS をディセーブルするには、auto qos コマンド インターフェイス コンフィギュレーション コマンドの **no** 形式（**no auto qos voip** など）を使用します。このポートに対して、自動 QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。自動 QoS をイネーブルにした最後のポートで、**no auto qos voip** コマンドを入力すると、自動 QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、自動 QoS はディセーブルとみなされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

no mls qos グローバル コンフィギュレーション コマンドを使用して、自動 QoS によって生成されたグローバル コンフィギュレーション コマンドをディセーブルにできます。QoS がディセーブルの場合、パケットが修正されなくなるため（パケットの CoS、DSCP、IP precedence の値は変更されない）、ポートの信頼性に関する概念はなくなります。トラフィックはパススルー モードでスイッチングされます（パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます）。

自動 QoS 情報の表示

初期自動 QoS 設定を表示するには、**show auto qos** [**interface** [*interface-id*]] 特権 EXEC コマンドを使用します。ユーザによる設定変更を表示するには、**show running-config** 特権 EXEC コマンドを使用します。**show auto qos** および **show running-config** コマンド出力を比較すると、ユーザが定義した QoS 設定を特定できます。

自動 QoS の影響を受ける可能性のある現在の QoS の設定情報を表示するには、次のいずれかのコマンドを使用します。

- **show mls qos**
- **show mls qos maps cos-dscp**
- **show mls qos interface** [*interface-id*] [**buffers** | **queueing**]
- **show mls qos maps** [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-output-q**]
- **show mls qos input-queue**
- **show running-config**

このコマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

標準 QoS の設定

標準 QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- 使用するアプリケーションのタイプおよびネットワークのトラフィック パターン
- トラフィックの特性およびネットワークのニーズ。バースト性の高いトラフィックかどうかの判別。音声およびビデオ ストリーム用の帯域幅確保の必要性
- ネットワークの帯域幅要件および速度
- ネットワーク上の輻輳発生箇所

ここでは、次の設定情報について説明します。

- 「標準 QoS のデフォルト設定」（P.37-36）
- 「標準 QoS 設定時の注意事項」（P.37-38）
- 「QoS のグローバルなイネーブル化」（P.37-41）（必須）
- 「VLAN ベース QoS の物理ポートでのイネーブル化」（P.37-41）（任意）
- 「ポートの信頼状態を使用した分類の設定」（P.37-42）（必須）
- 「QoS ポリシーの設定」（P.37-49）（必須）
- 「DSCP マップの設定」（P.37-76）（任意、DSCP/DSCP 変換マップまたはポリシング済み DSCP マップを使用する必要がない場合）
- 「入力キューの特性の設定」（P.37-82）（任意）
- 「出力キューの特性の設定」（P.37-86）（任意）

標準 QoS のデフォルト設定

QoS はディセーブルです。パケットが変更されない（パケット内の CoS、DSCP、および IP precedence 値は変更されない）ため、信頼できるポートまたは信頼できないポートといった概念は存在しません。トラフィックはパススルー モードでスイッチングされます（パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます）。

mls qos グローバル コンフィギュレーション コマンドを使用して QoS をイネーブルにし、その他のすべての QoS 設定がそれぞれのデフォルト値である場合、トラフィックはポリシングを伴わないベスト エフォート型として分類されます（DSCP および CoS 値は 0 に設定されます）。ポリシー マップは設定されません。すべてのポート上のデフォルト ポートの信頼性は、信頼性なし（untrusted）の状態です。デフォルトの入力キューおよび出力キューの設定については、「デフォルトの入力キュー設定」（P.37-36）および「デフォルトの出力キュー設定」（P.37-37）を参照してください。

デフォルトの入力キュー設定

表 37-6 に、QoS がイネーブルの場合のデフォルトの入力キュー設定を示します。

表 37-6　デフォルトの入力キュー設定

機能	キュー 1	キュー 2
バッファ割り当て	90%	10%
帯域幅割り当て [1]	4	4
プライオリティ キューの帯域幅 [2]	0	10
WTD ドロップしきい値 1	100%	100%
WTD ドロップしきい値 2	100%	100%

1. 帯域幅は各キューで平等に共有されます。SRR は共有モードでだけパケットを送信します。
2. キュー 2 はプライオリティ キューです。共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

表 37-7 に、デフォルトの QoS がイネーブルの場合の CoS 入力キューしきい値マップを示します。

表 37-7　デフォルトの CoS 入力キューのしきい値

CoS 値	キュー ID - しきい値 ID
0 ～ 4	1–1
5	2–1
6、7	1–1

表 37-8 に、デフォルトの QoS がイネーブルの場合の DSCP 入力キューしきい値マップを示します。

表 37-8　デフォルトの DSCP 入力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 ～ 39	1–1
40 ～ 47	2–1
48 ～ 63	1–1

デフォルトの出力キュー設定

表 37-9 に、QoS がイネーブルの場合の各キューセットのデフォルトの出力キュー設定を示します。すべてのポートはキューセット 1 にマッピングされます。ポートの帯域幅制限は 100% に設定され、レートは制限されません。

表 37-9　デフォルトの出力キュー設定

機能	キュー 1	キュー 2	キュー 3	キュー 4
バッファ割り当て	25%	25%	25%	25%
WTD ドロップしきい値 1	100%	200%	100%	100%
WTD ドロップしきい値 2	100%	200%	100%	100%
予約済みしきい値	50%	50%	50%	50%
最大しきい値	400%	400%	400%	400%
SRR シェーピング重み（絶対）[1]	25	0	0	0
SRR 共有重み [2]	25	25	25	25

1. シェーピング重みが 0 の場合、このキューは共有モードで動作します。
2. 帯域幅の 4 分の 1 が各キューに割り当てられます。

表 37-10 に、デフォルトの QoS がイネーブルの場合の CoS 出力キューしきい値マップを示します。

表 37-10　デフォルトの CoS 出力キューしきい値マップ

CoS 値	キュー ID - しきい値 ID
0、1	2–1
2、3	3–1
4	4–1
5	1–1
6、7	4–1

表 37-11 に、デフォルトの QoS がイネーブルの場合の DSCP 出力キューしきい値マップを示します。

表 37-11　デフォルトの DSCP 出力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 ～ 15	2–1
16 ～ 31	3–1
32 ～ 39	4–1
40 ～ 47	1–1
48 ～ 63	4–1

デフォルトのマッピング テーブル設定

デフォルトの CoS/DSCP マップは、表 37-12（P.37-76）のとおりです。

デフォルトの IP precedence/DSCP マップは、表 37-13（P.37-77）のとおりです。

デフォルトの DSCP/CoS マップは、表 37-14（P.37-79）のとおりです。

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

デフォルトのポリシング設定 DSCP マップは、着信 DSCP 値を（マークダウンしない）同じ DSCP 値にマッピングするヌル マップです。

標準 QoS 設定時の注意事項

QoS の設定を開始する前に、次の項の情報に注意してください。

- 「QoS ACL の注意事項」（P.37-38）
- 「IPv6 QoS ACL の注意事項」（P.37-38）
- 「インターフェイスでの QoS の適用」（P.37-38）
- 「IPv6 QoS のスイッチ スタックでの設定」（P.37-39）
- 「ポリシングの注意事項」（P.37-39）
- 「一般的な QoS の注意事項」（P.37-40）

QoS ACL の注意事項

ここでは、QoS アクセス コントロール リスト（ACL）の設定時の注意事項について説明します。

- IP フラグメントと設定されている IP 拡張 ACL を照合することによって、QoS を実施することはできません。IP フラグメントはベストエフォート型として送信されます。IP フラグメントは IP ヘッダーのフィールドで示されます。
- クラス マップごとにサポートされる ACL は 1 つだけです。また、クラス マップごとにサポートされる **match** クラス マップ コンフィギュレーション コマンドは 1 つだけです。ACL には、フィールドとパケットの内容を照合する ACE を複数指定できます。
- ポリシー マップの信頼ステートメントでは、ACL ラインごとに複数のハードウェア エントリが必要です。入力サービス ポリシー マップの ACL に信頼ステートメントが含まれている場合、アクセス リストが長くなりすぎて、使用できるハードウェア メモリに適せず、ポリシー マップをポートに適用するときにエラーが発生することがあります。QoS ACL のライスの数はできるだけ最小限に押さえてください。

IPv6 QoS ACL の注意事項

第 36 章「IPv6 ACL の設定」を参照してください。

インターフェイスでの QoS の適用

ここでは、QoS 物理ポートの設定時の注意事項について説明します。また、この説明は SVI（レイヤ 3 インターフェイス）にも適用されます。

- QoS は物理ポートおよび SVI で設定できます。物理ポートに QoS を設定する場合、非階層型ポリシー マップを作成および適用します。SVI に QoS を設定すると、非階層型および段階型ポリシー マップを作成および適用します。
- ブリッジング、ルーティング、または CPU への送信のいずれを行うかに関係なく、着信トラフィックは分類、ポリシング、およびマークダウンされます（設定されている場合）。ブリッジングされたフレームをドロップしたり、DSCP および CoS 値を変更することができます。

- ポリシー マップを物理ポートまたは SVI で設定するときは、次の注意事項に従ってください。
  - 物理ポートと SVI に同じポリシー マップを適用できません。
  - 物理ポートで VLAN ベースの QoS を設定した場合、スイッチはそのポートにあるすべてのポートベースのポリシー マップを削除します。そうすることで、物理ポートのトラフィックは、自身のポートの SVI に適用されているポリシー マップの適用を受け入れられます。
  - SVI に付加された階層型ポリシー マップでは、物理ポートのインターフェイス レベルで個々のポリサーだけを設定し、ポート上のトラフィックの帯域幅制限を指定できます。入力ポートは、トランクまたは静的アクセス ポートとして設定する必要があります。階層型ポリシー マップの VLAN レベルでは、ポリサーを設定できません。
  - スイッチは、階層型ポリシー マップの集約ポリサーをサポートしません。
  - 階層ポリシー マップを SVI に適用すると、インターフェイス レベル ポリシー マップを変更したり、階層ポリシー マップから削除することはできません。階層ポリシー マップに、新しいインターフェイス レベル ポリシー マップを追加することもできません。このような変更を行いたい場合は、まず階層ポリシー マップを SVI から削除する必要があります。また、階層型ポリシー マップで指定されたクラス マップを追加したり削除したりすることもできません。

IPv6 QoS のスイッチ スタックでの設定

Cisco IOS Release 12.2(52)SE 以降のリリースでは、IPv6 QoS をスイッチまたはスイッチ スタックでイネーブルにできます。スタックに Cisco 3560E および Cisco 3750E スイッチだけが含まれている場合、QoS 設定はすべてのトラフィックに適用されます。1 つ以上の Cisco Catalyst 3750 スイッチを含むスタックの IPv6 QoS に関する注意事項は、次のとおりです。

- 任意のスイッチをスタック マスターとして使用できます。
- IPv6 ACL を含むポリシーは、Cisco 3560E および 3750E スイッチ インターフェイスだけに適用できます。
- 付加されたポリシーを変更して、IPv6 ACL を Cisco 3560E および Cisco 3750E スイッチ インターフェイスだけに含めることができます。
- *match protocol IPv6* 分類を含むポリシーは、Cisco 3560E および Cisco 3750E スイッチ インターフェイスだけに適用されます。
- IPv4 および IPv6 の両方の分類を含む QoS ポリシーは、混合スイッチ スタックの SVI に付加できます。ただし、このポリシーは、Cisco 3750 スイッチ インターフェイスに入る IPv4 トラフィックだけ、および Cisco 3750E スイッチ インターフェイスの IPv4 および IPv6 トラフィックの両方に適用されます。
- IPv6 トラストは、Cisco 3750 および Cisco 3750E の両方のスイッチでサポートされます。
- IPv6 固有の分類（IPv6 ACL または **match protocol ipv6** コマンドなど）を含む QoS ポリシーは、Cisco 3750E インターフェイス、および任意の SVI（Cisco 3750E スイッチがスタックの一部である場合）でサポートされます。
- 共通の IPv4 および IPv6 分類を含む QoS ポリシーは、スタックのすべての Cisco 3750E インターフェイスでサポートされます。IPv4 分類だけがスタックの他方のスイッチでサポートされます。

ポリシングの注意事項

ポリシングの注意事項を次に示します。

- 複数の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個のシステムの内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。たとえば、32 のポリサーを

ギガビット イーサネット ポートで、7 のポリサーを 10 ギガビット イーサネット ポートで設定できます。または 64 のポリサーをギガビット イーサネット ポートで、4 のポリサーを 10 ギガビット イーサネット ポートで設定できます。ポリサーは必要に応じてソフトウェアによって割り当てられ、ハードウェアおよび ASIC 境界の制約を受けます。ポートごとにポリサーを確保することはできません。ポートがポリサーに割り当てられる保証はありません。

- 入力ポートでは、1 つのパケットにポリサーを 1 つだけ適用できます。設定できるのは平均速度および確定されたバースト パラメータだけです。
- 同じ非段階型ポリシー マップ内の複数のトラフィック クラスで共有される集約ポリサーを作成できます。ただし、集約ポリサーを異なるポリシー マップにわたって使用することはできません。
- QoS 対応として設定されているポートを介して受信したすべてのトラフィックは、そのポートに結合されたポリシー マップに基づいて分類、ポリシング、およびマーキングが行われます。QoS 対応として設定されているトランク ポートの場合、ポートを介して受信したすべての VLAN のトラフィックは、そのポートに結合されたポリシー マップに基づいて分類、ポリシング、およびマーキングが行われます。
- スイッチ上で EtherChannel ポートが設定されている場合、EtherChannel を形成する個々の物理ポートに QoS の分類、ポリシング、マッピング、およびキューイングを設定する必要があります。QoS 設定が EtherChannel のすべてのポートで一致する必要があるかどうかを決定してください。
- 既存の QoS ポリシーのポリシー マップを変更する必要がある場合は、まずすべてのインターフェイスからポリシー マップを削除した後、ポリシー マップを変更またはコピーします。変更を完了した後、変更されたポリシー マップをインターフェイスに適用します。すべてのインターフェイスからまずポリシー マップを削除しなければ、CPU 使用率が上昇し、それによってコンソールが非常に長い時間、一時停止するおそれがあります。

一般的な QoS の注意事項

一般的な QoS の注意事項を次に示します。

- スイッチで受信された制御トラフィック（スパニングツリー Bridge Protocol Data Unit [BPDU; ブリッジ プロトコル データ ユニット] やルーティング アップデート パケットなど）には、入力 QoS 処理がすべて行われます。
- キュー設定を変更すると、データが失われることがあります。したがって、トラフィックが最小のときに設定を変更するようにしてください。
- IP サービス フィーチャ セットを実行しているスイッチは、Policy-Based Routing（PBR; ポリシーベース ルーティング）ルート マップで QoS DSCP および IP precedence マッチングをサポートします。ただし次の制限があります。
  - QoS DSCP 変換マップと PBR ルート マップを同じインターフェイスには適用できません。
  - 透過的な DSCP と PBR DSCP ルート マップは同じスイッチでは設定できません。

QoS のグローバルなイネーブル化

デフォルトでは、QoS はスイッチ上でディセーブルに設定されています。Cisco IOS Release 12.2(52)SE 以降のリリースでは、IPv6 QoS がサポートされます。IPv6 QoS をスイッチでイネーブルにするには、デュアル IP SDM テンプレートを設定して、スイッチをリロードする必要があります。このテンプレートは、IPv4 および IPv6 QoS の両方の設定をイネーブルにします。

QoS をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos**	QoS をグローバルにイネーブルにします。 デフォルト設定における QoS の動作については、「標準 QoS のデフォルト設定」（P.37-36）、「入力キューのキューイングおよびスケジューリング」（P.37-16）、および「出力キューのキューイングおよびスケジューリング」（P.37-18）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

QoS をディセーブルにするには、**no mls qos** グローバル コンフィギュレーション コマンドを使用します。

VLAN ベース QoS の物理ポートでのイネーブル化

デフォルトでは、VLAN ベース QoS はすべての物理スイッチ ポートでディセーブルです。スイッチは、クラス マップやポリシー マップなど QoS を物理ポートだけに基づいて適用します。Cisco IOS Release 12.2(25)SE 以降のリリースでは、VLAN ベース QoS をスイッチ ポートでイネーブルにできます。

VLAN ベース QoS をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は、SVI の段階型ポリシー マップのインターフェイス レベルで指定される物理ポートで必要です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**mls qos vlan-based**	ポート上で VLAN ベース QoS をイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** *interface-id*	VLAN ベース QoS が物理ポートでイネーブルになっていることを確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN ベース QoS を物理ポートでディセーブルにするには、**no mls qos vlan-based** インターフェイス コンフィギュレーション コマンドを使用します。

ポートの信頼状態を使用した分類の設定

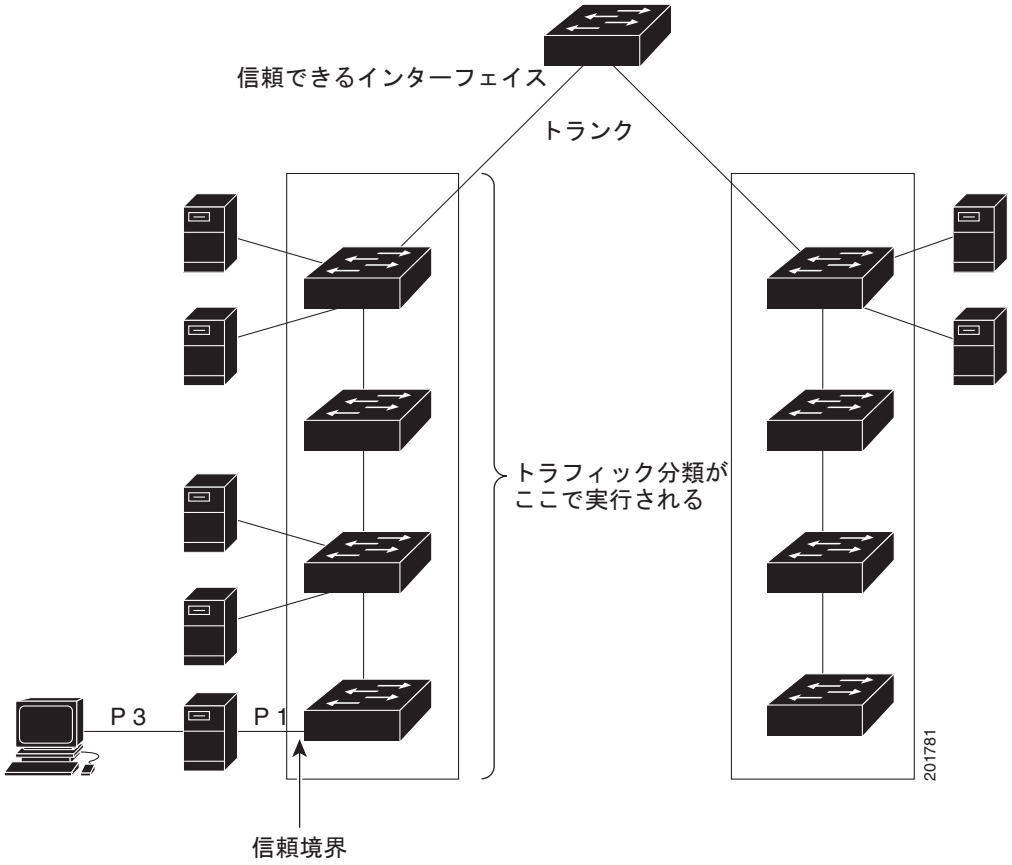
ここでは、ポートの信頼状態を使用して着信トラフィックを分類する方法について説明します。ネットワーク設定に応じて、次に示す作業または「QoS ポリシーの設定」（P.37-49）に記載されている作業を 1 つ以上実行する必要があります。

- 「QoS ドメイン内のポートの信頼状態の設定」（P.37-42）
- 「インターフェイスの CoS 値の設定」（P.37-44）
- 「ポート セキュリティを確保するための信頼境界機能の設定」（P.37-45）
- 「DSCP 透過モードのイネーブル化」（P.37-46）
- 「別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定」（P.37-47）

QoS ドメイン内のポートの信頼状態の設定

QoS ドメインに入るパケットは、QoS ドメインのエッジで分類されます。パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないため、QoS ドメイン内のスイッチ ポートはいずれか 1 つの信頼状態に設定できます。図 37-11 に、ネットワーク トポロジの例を示します。

図 37-11　QoS ドメイン内のポートの信頼状態



ポートが受信したトラフィックの分類を信頼するようにポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	信頼するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。

	コマンド	目的
ステップ 3	**mls qos trust** [**cos** | **dscp** | **ip-precedence**]	ポートの信頼状態を設定します。 デフォルトでは、ポートは trusted ではありません。キーワードを指定しない場合、デフォルトは **dscp** です。 キーワードの意味は次のとおりです。 • **cos**：パケットの CoS 値を使用して入力パケットを分類します。タグのない非 IP パケットの場合、デフォルト ポートの CoS 値が使用されます。デフォルト ポート CoS 値は 0 です。 • **dscp**：パケットの DSCP 値を使用して入力パケットを分類します。非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルト ポート CoS が使用されます。スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。 • **ip-precedence**：パケットの IP precedence 値を使用して入力パケットを分類します。非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルト ポート CoS が使用されます。スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

untrusted ステートにポートを戻す場合は、**no mls qos trust** インターフェイス コンフィギュレーション コマンドを使用します。

デフォルト CoS 値を変更する方法については、「インターフェイスの CoS 値の設定」（P.37-44）を参照してください。CoS/DSCP マップを設定する方法については、「CoS/DSCP マップの設定」（P.37-76）を参照してください。

インターフェイスの CoS 値の設定

QoS は、trusted ポートおよび untrusted ポートで受信したタグなしフレームに、**mls qos cos** インターフェイス コンフィギュレーション コマンドで指定された CoS 値を割り当てます。

ポートのデフォルト CoS 値を定義したり、デフォルト CoS 値をポートのすべての着信パケットに割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。

	コマンド	目的
ステップ 3	**mls qos cos** {*default-cos* | **override**}	デフォルトのポート CoS 値を設定します。 • *default-cos* には、ポートに割り当てるデフォルト CoS 値を指定します。パケットがタグなしの場合、デフォルト CoS 値がパケットの CoS 値になります。指定できる CoS 範囲は 0 ～ 7 です。デフォルト値は 0 です。 • 着信パケットにすでに設定されている信頼状態を上書きし、すべての着信パケットにデフォルト ポート CoS 値を適用する場合は、**override** キーワードを使用します。デフォルトでは、CoS の上書きはディセーブルに設定されています。 特定のポートに届くすべての着信パケットに、他のポートからのパケットより高いプライオリティを与える場合には、**override** キーワードを使用します。ポートが DSCP、CoS、または IP precedence を信頼するように設定されている場合も、このコマンドを実行すると設定済みの信頼状態が上書きされ、すべての着信 CoS 値に、このコマンドによって設定されたデフォルト CoS 値が割り当てられます。着信パケットがタグ付きの場合、パケットの CoS 値は、出力ポートで、ポートのデフォルト CoS を使用して変更されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻す場合は、**no mls qos cos** {*default-cos* | **override**} インターフェイス コンフィギュレーション コマンドを使用します。

ポート セキュリティを確保するための信頼境界機能の設定

一般的なネットワークでは、Cisco IP Phone をスイッチ ポートに接続して（図 37-11（P.37-43）を参照）、電話の背後からデータ パケットを生成するデバイスをカスケードします。Cisco IP Phone では、音声パケット CoS レベルをハイ プライオリティ（CoS = 5）にマーキングし、データ パケットをロープライオリティ（CoS = 0）にマーキングすることで、共有データ リンクを通して音声品質を保証しています。電話からスイッチに送信されたトラフィックは通常 802.1Q ヘッダーを使用するタグでマーキングされています。このヘッダーには VLAN 情報、およびパケットのプライオリティを示すサービス クラス（CoS）の 3 ビットフィールドが格納されます。

ほとんどの Cisco IP Phone 設定では、電話からスイッチへ送信されるトラフィックは、音声トラフィックがネットワーク内の他のタイプのトラフィックに対して適切にプライオリティ付けがされていることを保証するように信頼されています。**mls qos trust cos** インターフェイス コンフィギュレーション コマンドを使用して、ポートで受信されるすべてのトラフィックの CoS ラベルを信頼するように、電話が接続されているスイッチ ポートを設定します。**mls qos trust dscp** インターフェイス コンフィギュレーション コマンドを使用して、ポートで受信されるすべてのトラフィックの DSCP ラベルを信頼するように、電話が接続されているルーテッド ポートを設定します。

信頼設定により、ユーザが電話をバイパスして PC を直接スイッチに接続する場合に、ハイ プライオリティ キューの誤使用を避けるのにも信頼境界機能を使用できます。信頼境界機能を使用しないと、（信頼性のある CoS 設定により）PC が生成した CoS ラベルがスイッチで信頼されてしまいます。それに対して、信頼境界機能は CDP を使用してスイッチ ポートにある Cisco IP Phone（Cisco IP Phone 7910、7935、7940、および 7960）の存在を検出します。電話が検出されない場合、信頼境界機能がハイ プライオリティ キューの誤使用を避けるためにスイッチ ポートの信頼設定をディセーブルにします。信頼境界機能は、PC および Cisco IP Phone がスイッチに接続されているハブに接続されている場合は機能しないことに注意してください。

場合によっては、Cisco IP Phone に接続された PC がハイプライオリティのデータ キューを利用しないように設定できます。**switchport priority extend cos** インターフェイス コンフィギュレーション コマンドを使用して、PC から受信するトラフィックのプライオリティを上書きするようにスイッチ CLI を介して電話を設定できます。

信頼境界機能をポート上でイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cdp run**	CDP をグローバルにイネーブルにします。デフォルトでは、CDP がイネーブルに設定されています。
ステップ 3	**interface** *interface-id*	Cisco IP Phone に接続するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 4	**cdp enable**	ポート上で CDP をイネーブルに設定します。デフォルトでは、CDP がイネーブルに設定されています。
ステップ 5	**mls qos trust cos**	Cisco IP Phone から受信したトラフィックの CoS 値を信頼するように、スイッチ ポートを設定します。 または
	mls qos trust dscp	Cisco IP Phone から受信したトラフィックの DSCP 値を信頼するように、ルーテッド ポートを設定します。 デフォルトでは、ポートは trusted ではありません。
ステップ 6	**mls qos trust device cisco-phone**	Cisco IP Phone が信頼性のあるデバイスであることを指定します。 信頼境界機能と自動 QoS（**auto qos voip** インターフェイス コンフィギュレーション コマンド）を同時にイネーブルにはできません。両者は相互に排他的です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show mls qos interface**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

信頼境界機能をディセーブルにするには、**no mls qos trust device** インターフェイス コンフィギュレーション コマンドを使用します。

DSCP 透過モードのイネーブル化

スイッチでは、透過的な DSCP 機能がサポートされています。この機能は発信パケットの DSCP フィールドだけに作用します。デフォルトでは、DSCP 透過性はディセーブルです。スイッチでは着信パケットの DSCP フィールドが変更され、発信パケットの DSCP フィールドは、ポートの信頼設定、ポリシングとマーキング、DSCP/DSCP 変換マップを含めて QoS（Quality of Service）に基づきます。

no mls qos rewrite ip dscp コマンドを用いて 透過的な DSCP 機能をイネーブルにした場合、スイッチは着信パケットの DSCP フィールドは変更せず、送信パケットの DSCP フィールドも着信パケットのものと同じになります。

（注）　透過的な DSCP 機能をイネーブルにしても、IEEE 802.1Q トンネリング ポート上のポート信頼性の設定には影響しません。

DSCP 透過設定に関係なく、スイッチはパケットの内部 DSCP 値を変更し、この内部 DSCP 値を使用して、スイッチはトラフィックのプライオリティを表すサービス クラス（CoS）値を生成します。また、スイッチは内部 DSCP 値を使用して、出力キューおよびしきい値を選択します。

特権 EXEC モードを開始して、透過的な DSCP 機能をスイッチでイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos**	QoS をグローバルにイネーブルにします。
ステップ 3	**no mls qos rewrite ip dscp**	透過的な DSCP 機能をイネーブルにします。スイッチが IP パケットの DSCP フィールドを変更しないよう設定されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

透過的な DSCP 機能をディセーブルにして、信頼設定または ACL に基づいてスイッチに DSCP 値を変更させる設定にするには、**mls qos rewrite ip dscp** グローバル コンフィギュレーション コマンドを使用します。

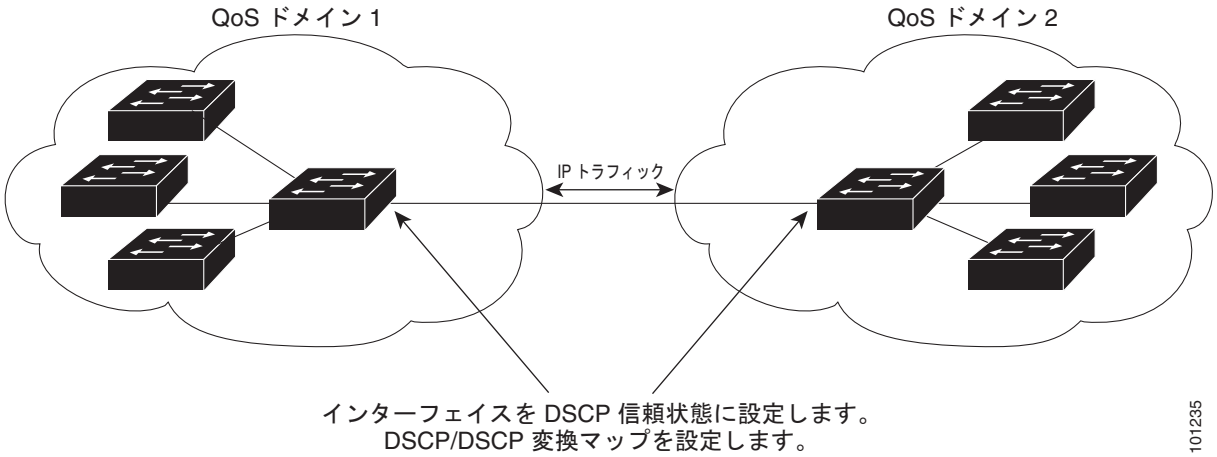
no mls qos グローバル コンフィギュレーション コマンドで、QoS をディセーブルにした場合、CoS および DSCP 値は変更されません（デフォルトの QoS 設定）。

no mls qos rewrite ip dscp グローバル コンフィギュレーション コマンドを入力して DSCP 透過をイネーブルにしてから、**mls qos trust** [**cos** | **dscp**] インターフェイス コンフィギュレーション コマンドを入力した場合、DSCP 透過はイネーブルのままとなります。

別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定

2 つの異なる QoS ドメインを管理しているときに、その QoS ドメイン間の IP トラフィックに QoS 機能を実装する場合は、ドメインの境界に位置するスイッチ ポートを DSCP trusted ステートに設定できます（図 37-12 を参照）。それにより、受信ポートでは DSCP trusted 値をそのまま使用し、QoS の分類手順が省略されます。2 つのドメインで異なる DSCP 値が使用されている場合は、他のドメイン内での定義に一致するように一連の DSCP 値を変換する DSCP/DSCP 変換マップを設定できます。

図 37-12　別の QoS ドメインとの境界ポートの DSCP 信頼状態



ポート上に DSCP trusted ステートを設定して、DSCP/DSCP 変換マップを変更するには、特権 EXEC モードで次の手順を実行します。両方の QoS ドメインに一貫した方法でマッピングするには、両方のドメイン内のポート上で次の手順を実行する必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*	DSCP/DSCP 変換マップを変更します。 デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。 • *dscp-mutation-name* には、変換マップ名を入力します。新しい名前を指定することにより、複数のマップを作成できます。 • *in-dscp* には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *out-dscp* には、1 つの DSCP 値を入力します。 DSCP の範囲は 0 ～ 63 です。
ステップ 3	**interface** *interface-id*	信頼するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 4	**mls qos trust dscp**	DSCP trusted ポートとして入力ポートを設定します。デフォルトでは、ポートは trusted ではありません。
ステップ 5	**mls qos dscp-mutation** *dscp-mutation-name*	指定された DSCP trusted 入力ポートにマップを適用します。 *dscp-mutation-name* には、ステップ 2 で作成した変換マップ名を指定します。 1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show mls qos maps dscp-mutation**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

non-trusted ステートにポートを戻す場合は、**no mls qos trust** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトの DSCP/DSCP 変換マップ値に戻すには、**no mls qos map dscp-mutation** *dscp-mutation-name* グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP を信頼する状態にポートを設定して、着信した DSCP 値 10 ～ 13 が DSCP 値 30 にマッピングされるように DSCP/DSCP 変換マップ（*gi1/0/2-mutation*）を変更する例を示します。

```
Switch(config)# mls qos map dscp-mutation gigabitethernet1/0/2-mutation 10 11 12 13 to 30
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation gigabitethernet1/0/2-mutation
Switch(config-if)# end
```

QoS ポリシーの設定

通常の場合、QoS ポリシーを設定するには、トラフィックをクラスに分類したり、これらのトラフィック クラスに適用されるポリシーを設定したり、ポリシーをポートに付加したりする必要があります。

基本情報については、「分類」（P.37-5）および「ポリシングおよびマーキング」（P.37-9）を参照してください。設定時の注意事項については、「標準 QoS 設定時の注意事項」（P.37-38）を参照してください。

ここでは、トラフィックを分類、ポリシング、マーキングする方法について説明します。ネットワーク設定に応じて、次の作業を 1 つ以上実行する必要があります。

- 「ACL を使用したトラフィックの分類」（P.37-50）
- 「クラス マップを使用したトラフィックの分類」（P.37-55）
- 「クラス マップの使用および IPv6 トラフィックのフィルタリングによるトラフィックの分類」（P.37-59）
- 「ポリシー マップを使用した物理ポートのトラフィックの分類、ポリシング、およびマーキング」（P.37-61）
- 「階層型ポリシー マップを使用した SVI のトラフィックの分類、ポリシング、およびマーキング」（P.37-66）
- 「集約ポリサーを使用したトラフィックの分類、ポリシング、およびマーキング」（P.37-74）

ACL を使用したトラフィックの分類

入力 IP トラフィックを分類するには、IP 標準または IP 拡張 ACL を使用します。Cisco IOS Release 12.2(52)SE 以降のリリースでは、IPv6 ACL を使用できます。レイヤ 2 MAC ACL を使用して、非 IP トラフィックを分類することもできます。

IP トラフィック用の IP 標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	IP 標準 ACL を作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* には、アクセス リスト番号を入力します。有効範囲は 1 ～ 99 および 1300 ～ 1999 です。 • **permit** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを許可します。**deny** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 • *source* には、パケットの送信元となるネットワークまたはホストを指定します。**any** キーワードは 0.0.0.0 255.255.255.255 の省略形として使用できます。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 **（注）** アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。

次に、指定された 3 つのネットワーク上のホストだけにアクセスを許可する例を示します。ネットワーク アドレスのホスト部分にワイルドカード ビットが適用されます。アクセス リストのステートメントと一致しない送信元アドレスのホストはすべて拒否されます。

```
Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
! (Note: all other access implicitly denied)
```

IP トラフィック用の IP 拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*	IP 拡張 ACL を作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* には、アクセス リスト番号を入力します。有効範囲は 100 ～ 199 および 2000 ～ 2699 です。 • **permit** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを許可します。**deny** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 • *protocol* には、IP プロトコルの名前または番号を入力します。疑問符（?）を使用すると、使用できるプロトコル キーワードのリストが表示されます。 • *source* には、パケットの送信元となるネットワークまたはホストを指定します。ネットワークまたはホストを指定するには、ドット付き 10 進表記を使用したり、*source* 0.0.0.0 *source-wildcard* 255.255.255.255 の短縮形として **any** キーワードを使用したり、*source* 0.0.0.0 を表す **host** キーワードを使用したりします。 • *source-wildcard* では、無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。ワイルドカードを指定するには、ドット付き 10 進表記を使用したり、*source* 0.0.0.0 *source-wildcard* 255.255.255.255 の短縮形として **any** キーワードを使用したり、*source* 0.0.0.0 を表す **host** キーワードを使用します。 • *destination* には、パケットの宛先となるネットワークまたはホストを指定します。*destination* および *destination-wildcard* には、*source* および *source-wildcard* での説明と同じオプションを使用できます。 **（注）** アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。

次に、任意の送信元から、DSCP 値が 32 に設定されている任意の宛先への IP トラフィックを許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip any any dscp 32
```

次に、10.1.1.1 の送信元ホストから 10.1.1.2 の宛先ホストへの IP トラフィック（precedence 値は 5）を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
```

次に、任意の送信元からアドレス 224.0.0.2 の宛先グループへの PIM トラフィック（DSCP 値は 32）を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 102 permit pim any 224.0.0.2 dscp 32
```

IP トラフィック用の IPv6 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 access-list** *access-list-name*	IPv6 ACL を作成し、IPv6 アクセスリスト コンフィギュレーション モードを開始します。 アクセス リスト名にはスペースまたは引用符を含めることはできません。また、数字で開始することもできません。

	コマンド	目的
ステップ 3	{**deny** | **permit**} *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/ prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]	**deny** または **permit** を入力し、条件と一致した場合にパケットを拒否するか、または許可するかを指定します。次に、条件について説明します。 • *protocol* には、インターネット プロトコルの名前、**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**stcp**、**tcp**、または **udp**、あるいは IPv6 プロトコル番号を示す 0 ～ 255 の範囲の整数を入力します。 （注）　ICMP、TCP および UDP の追加パラメータについては、「IPv6 ACL の作成」（P.36-6）を参照してください。 • *source-ipv6-prefix/prefix-length* または *destination-ipv6-prefix/ prefix-length* は、コロン間で 16 ビット値を使用して 16 進数で指定された deny または permit 条件を設定するネットワークの発信元 / 宛先 IPv6 ネットワークまたはクラスです（RFC 2373 を参照してください）。 • IPv6 プレフィクス ::/0 の省略形として、**any** を使用できます。 • **host** *source-ipv6-address* または *destination-ipv6-address* には、コロン間に 16 ビット値を使用して 16 進数で指定された deny または permit 条件を設定する発信元 / 宛先 IPv6 ホストアドレスを入力します。 • （任意）*operator* には、指定されたプロトコルの送信元または宛先ポートを比較するオペランドを指定します。オペランドは、**lt**（less than：未満）、**gt**（greater than：より大きい）、**eq**（equal：一致）、**neq**（not equal：不一致）、**range** です。 *source-ipv6-prefix/prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。*destination-ipv6-prefix/prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 • （任意）*port-number* に 10 進数（0 ～ 65535）として入力するか、TCP または UDP ポート名を入力します。TCP ポート名は TCP をフィルタリングする場合にだけ使用できます。UDP ポート名は UDP をフィルタリングする場合にだけ使用できます。 • （任意）**dscp** *value* を入力して、各 IPv6 パケット ヘッダーのトラフィック クラス フィールドのトラフィック クラス値と Differentiated Services Code Point 値を照合します。指定できる範囲は 0 ～ 63 です。 • （任意）先頭以外のフラグメントをチェックするには、**fragments** を入力します。このキーワードが表示されるのは、プロトコルが **ipv6** の場合だけです。 • （任意）エントリと一致するパケットについてのログ メッセージをコンソールに送信するには、**log** を入力します。入力インターフェイスをログ エントリに含めるには、**log-input** を入力します。ロギングはルータ ACL だけでサポートされます。 • （任意）IPv6 パケットがルーティングされるように指定するには、**routing** を入力します。

	コマンド	目的
		（続き） • （任意）アクセス リスト ステートメントのシーケンス番号を指定するには、**sequence** *value* を入力します。指定できる範囲は 1 ～ 4294967295 です。 • （任意）deny または permit ステートメントに適用される時間範囲を指定するには、**time-range** *name* を入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 access-list**	アクセス リストの設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、**no ipv6 access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。

次に、任意の送信元から、DSCP 値が 32 に設定されている任意の宛先への IPv6 トラフィックを許可する ACL を作成する例を示します。

```
Switch(config)# ipv6 access-list 100 permit ip any any dscp 32
```

次に、10.1.1.1 の送信元ホストから 10.1.1.2 の宛先ホストへの IPv6 トラフィック（precedence 値は 5）を許可する ACL を作成する例を示します。

```
Switch(config)# ipv6 access-list ipv6_Name_ACL permit ip host 10::1 host 10.1.1.2
precedence 5
```

非 IP トラフィック用のレイヤ 2 MAC ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac access-list extended** *name*	リスト名を指定し、レイヤ 2 MAC ACL を作成します。 このコマンドを入力すると、拡張 MAC ACL コンフィギュレーション モードに切り替わります。

	コマンド	目的
ステップ 3	{**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]	条件が一致した場合に許可または拒否するトラフィック タイプを指定します。必要な回数だけコマンドを入力します。 • *src-MAC-addr* には、パケットの送信元となるホストの MAC アドレスを指定します。MAC アドレスを指定するには、16 進表記（H.H.H）を使用したり、*source* 0.0.0、*source-wildcard* ffff.ffff.ffff の短縮形として **any** キーワードを使用したり、*source* 0.0.0 を表す **host** キーワードを使用したりします。 • *mask* では、無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。 • *dst-MAC-addr* には、パケットの宛先となるホストの MAC アドレスを指定します。MAC アドレスを指定するには、16 進表記（H.H.H）を使用したり、*source* 0.0.0、*source-wildcard* ffff.ffff.ffff の短縮形として **any** キーワードを使用したり、*source* 0.0.0 を表す **host** キーワードを使用したりします。 • （任意）*type mask* には、Ethernet II または SNAP でカプセル化されたパケットの Ethertype 番号を指定して、パケットのプロトコルを識別します。*type* の範囲は 0 ～ 65535 です。通常は 16 進数で指定します。*mask* には、一致をテストする前に Ethertype に適用される*無視（don't care）*ビットを入力します。 **（注）** アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*access-list-number* | *access-list-name*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、**no mac access-list extended** *access-list-name* グローバル コンフィギュレーション コマンドを使用します。

次に、2 つの許可（permit）ステートメントを指定したレイヤ 2 の MAC ACL を作成する例を示します。最初のステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。2 番めのステートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、Ethertype が XNS-IDP のトラフィックだけが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
! (Note: all other access implicitly denied)
```

クラス マップを使用したトラフィックの分類

特定のトラフィック フロー（またはクラス）を他のすべてのトラフィックから分離して名前を付けるには、**class-map** グローバル コンフィギュレーション コマンドを使用します。クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。match ステー

トメントには、ACL、IP precedence 値、DSCP 値などの条件を指定できます。一致条件は、クラス マップ コンフィギュレーション モードで 1 つの一致ステートメントを入力することによって定義されます。

（注）　**class** ポリシー マップ コンフィギュレーション コマンドを使用することによって、ポリシー マップの作成時にクラス マップを作成することもできます。詳細については、「ポリシー マップを使用した物理ポートのトラフィックの分類、ポリシング、およびマーキング」（P.37-61）および「階層型ポリシー マップを使用した SVI のトラフィックの分類、ポリシング、およびマーキング」（P.37-66）を参照してください。

クラス マップを作成し、トラフィックを分類するための一致条件を定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] または **access-list** *access-list-number* {**deny** | **permit**} *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] または **ipv6 access-list** *access-list-name* {**deny** | **permit**} *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/ prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] または **mac access-list extended** *name* {**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]	IP トラフィック用の IP 標準または IP 拡張 ACL または IPv6 ACL、あるいは非 IP トラフィック用のレイヤ 2 MAC ACL を作成し、必要な回数だけコマンドを繰り返します。 詳細については、「ACL を使用したトラフィックの分類」（P.37-50）を参照してください。 （注）　アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

	コマンド	目的
ステップ 3	**class-map** [**match-all** | **match-any**] *class-map-name*	クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 • （任意）このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、**match-all** キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • （任意）このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、**match-any** キーワードを使用します。この場合は、1 つ以上の一致条件と一致する必要があります。 • *class-map-name* には、クラス マップ名を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 **（注）** クラス マップごとにサポートされる **match** コマンドは 1 つだけのため、**match-all** でも **match-any** でもキーワードの機能は変わりません。**match-all** および **match-any** キーワードの使用に関する制限事項については、「名前付き標準および拡張 ACL の作成」（P.35-15）を参照してください。
ステップ 4	**match protocol** [*ip* | *ipv6*]	（任意）クラス マップが適用される IP プロトコルを指定します。 • IPv4 トラフィックを指定するには引数 *ip* を使用し、IPv6 トラフィックを指定するには *ipv6* を使用します。 • **match protocol** コマンドを使用する場合、**match-all** キーワードだけが **class-map** コマンドでサポートされます。 **（注）** このコマンドは、デュアル IPv4/IPv6 SDM テンプレートが設定されている場合だけ使用できます。 **match protocol** コマンドは、**match ip dscp** または **match precedence** コマンドと使用できますが、**match access-group** コマンドとは使用できません。 **match protocol** コマンドの詳細については、『*Cisco IOS Quality of Service Solutions Command Reference*』を参照してください。

	コマンド	目的
ステップ 5	**match** {**access-group** *acl-index-or-name* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}	トラフィックを分類するための一致条件を定義します。 デフォルトでは、一致条件は定義されていません。 クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。 • **access-group** *acl-index-or-name* には、ステップ 2 で作成した ACL の番号または名前を指定します。 • **match access-group** コマンドを使用して IPv6 トラフィックをフィルタリングするには、ステップ 2 で説明されているように IPv6 ACL を作成します。 • **ip dscp** *dscp-list* には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *ip-precedence-list* には、着信パケットと照合する IP precedence 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show class-map**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除するには、**no class-map** [**match-all** | **match-any**] *class-map-name* グローバル コンフィギュレーション コマンドを使用します。一致条件を削除するには、**no match** {**access-group** *acl-index-or-name* | **ip dscp** | **ip precedence**} クラス マップ コンフィギュレーション コマンドを使用します。

次に、*class1* というクラス マップの設定例を示します。*class1* にはアクセス リスト 103 という一致条件が 1 つ設定されています。このクラス マップによって、任意のホストから任意の宛先へのトラフィック（DSCP 値は 10）が許可されます。

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# end
Switch#
```

次に、DSCP 値が 10、11、12 である着信トラフィックとの一致を調べる、*class2* という名前のクラス マップを作成する例を示します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# end
Switch#
```

次に、IP-precedence 値が 5、6、7 である着信トラフィックとの一致を調べる、*class3* という名前のクラス マップを作成する例を示します。

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# end
Switch#
```

クラス マップの使用および IPv6 トラフィックのフィルタリングによるトラフィックの分類

Cisco IOS Release 12.2(52)SE 以降のリリースでは、スイッチは、デュアル IPv4/IPv6 SDM テンプレートが設定されている場合、IPv4 および IPv6 QoS の両方のトラフィックがサポートされます。デュアル IP SDM テンプレートが設定されている場合、**match ip dscp** および **match ip precedence** 分類は、IPv4 および IPv6 の両方のトラフィックと一致します。**match protocol** コマンドを使用すると、IP バージョン（IPv4 または IPv6）によりトラフィックをフィルタリングするセカンダリ一致分類を作成できます。

プライマリ一致基準を IPv4 トラフィックだけに適用するには、**match protocol** コマンドを **ip** キーワードを指定して使用します。プライマリ一致基準を IPv6 トラフィックだけに適用するには、**match protocol** コマンドを **ipv6** キーワードを指定して使用します。**match protocol** コマンドの詳細については、『*Cisco IOS Quality of Service Solutions Command Reference*』を参照してください。

クラス マップを作成し、トラフィックを分類し、IPv6 トラフィックをフィルタリングするための一致条件を定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** {**match-all**} *class-map-name*	クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 **match protocol** コマンドを使用する場合、**match-all** キーワードだけがサポートされます。 • *class-map-name* には、クラス マップ名を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。
ステップ 3	**match protocol** [*ip* | *ipv6*]	（任意）クラス マップが適用される IP プロトコルを指定します。 • IPv4 トラフィックを指定するには引数 *ip* を使用し、IPv6 トラフィックを指定するには *ipv6* を使用します。 • **match protocol** コマンドを使用する場合、**match-all** キーワードだけが **class-map** コマンドでサポートされます。 **（注）** このコマンドは、デュアル IPv4/IPv6 SDM テンプレートが設定されている場合だけ使用できます。 **match protocol** コマンドの詳細については、『*Cisco IOS Quality of Service Solutions Command Reference*』を参照してください。
ステップ 4	**match** {**ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}	トラフィックを分類するための一致条件を定義します。 デフォルトでは、一致条件は定義されていません。 • **ip dscp** *dscp-list* には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *ip-precedence-list* には、着信パケットと照合する IP precedence 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 6	**show class-map**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除するには、**no class-map** [**match-all** | **match-any**] *class-map-name* グローバル コンフィギュレーション コマンドを使用します。一致条件を削除するには、**no match** {**access-group** *acl-index-or-name* | **ip dscp** | **ip precedence**} クラス マップ コンフィギュレーション コマンドを使用します。

次に、IP DSCP および IPv6 と照合するクラス マップを設定する例を示します。

```
Switch(config)# class-map cm-1
Switch(config-cmap)# match ip dscp 10
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)# class-map cm-2
Switch(config-cmap)# match ip dscp 20
Switch(config-cmap)# match protocol ip
Switch(config-cmap)# exit
Switch(config)# policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G1/0/1
Switch(config-if)# service-policy input pm1
```

次に、IPv4 および IPv6 の両方のトラフィックに適用されるクラス マップを設定する例を示します。

```
Switch(config)# ip access-list 101 permit ip any any
Switch(config)# ipv6 access-list ipv6-any permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-2
Switch(config-cmap)# match access-group name ipv6-any
Switch(config-cmap)# exit
Switch(config)# Policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G0/1
Switch(config-if)# switch mode access
Switch(config-if)# service-policy input pm1
```

ポリシー マップを使用した物理ポートのトラフィックの分類、ポリシング、およびマーキング

作用対象となるトラフィック クラスを指定する非段階型ポリシー マップを、物理ポート上に設定できます。アクションには、トラフィック クラスの CoS、DSCP、または IP precedence 値を信頼するアクション、トラフィック クラスに特定の DSCP または IP precedence 値を設定するアクション、または一致した各トラフィック クラスのトラフィック帯域幅制限（ポリサー）およびトラフィックが適合しない場合のアクション（マーキング）などを指定できます。

ポリシー マップには、次の特性もあります。

- 1 つのポリシー マップに、それぞれ異なる一致条件とポリサーを指定した複数のクラス ステートメントを指定できます。
- ポリシー マップには、事前に設定されたデフォルトのトラフィック クラスをマップの最後に明示的に配置して指定することができます。
- 1 つのポートから受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。

ポリシー マップを物理ポートで設定するときは、次の注意事項に従ってください。

- 入力ポートごとに付加できるポリシー マップは、1 つだけです。
- **mls qos map ip-prec-dscp** *dscp1...dscp8* グローバル コンフィギュレーション コマンドを使用して IP-precedence/DSCP マップを設定する場合、その設定は IP precedence 値を信頼するよう設定されている入力インターフェイス上のパケットにだけ影響を与えます。ポリシー マップでは、**set ip precedence** *new-precedence* ポリシーマップ クラス コンフィギュレーション コマンドを使用してパケット IP precedence 値に新規の値を設定すると、出力 DSCP 値は IP precedence/DSCP マップからは影響を受けません。出力 DSCP 値を入力値とは異なる値に設定する場合、**set dscp** *new-dscp* ポリシー マップ クラス コンフィギュレーション コマンドを使用します。
- **set ip dscp** コマンドを入力または使用すると、スイッチによってこのコマンドがスイッチ コンフィギュレーションの **set dscp** に変更されます。
- パケット IP precedence 値を変更するには、**set ip precedence** または **set precedence** ポリシー マップ クラス コンフィギュレーション コマンドを使用できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。
- ポートに定義される各クラスの個別のセカンド レベル ポリシー マップを設定できます。セカンド レベル ポリシー マップは、各トラフィック クラスで作用するポリシング アクションを指定します。階層型ポリシー マップの設定については、「階層型ポリシー マップを使用した SVI のトラフィックの分類、ポリシング、およびマーキング」（P.37-66）を参照してください。
- **class class-default** ポリシーマップ コンフィギュレーション コマンドを使用してデフォルトのトラフィック クラスを設定すると、未分類のトラフィック（トラフィック クラスで指定された一致基準を満たさないトラフィック）は、デフォルトのトラフィック クラス（**class-default**）として処理されます。

非階層型ポリシー マップを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** [**match-all** | **match-any**] *class-map-name*	クラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 • （任意）このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、**match-all** キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • （任意）このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、**match-any** キーワードを使用します。この場合は、1 つ以上の一致条件と一致する必要があります。 • *class-map-name* には、クラス マップ名を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 **（注）** クラス マップごとにサポートされる **match** コマンドは 1 つだけのため、**match-all** でも **match-any** でもキーワードの機能は変わりません。**match-all** および **match-any** キーワードの使用に関する制限事項については、「名前付き標準および拡張 ACL の作成」（P.35-15）を参照してください。
ステップ 3	**policy-map** *policy-map-name*	ポリシー マップ名を入力することによってポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されていません。 ポリシー マップのデフォルト動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。
ステップ 4	**class** [*class-map-name* | **class-default**]	トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップのクラス マップは定義されていません。 すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。 **class-default** トラフィック クラスは、事前に定義されており、任意のポリシーに追加できます。このクラスは、常にポリシー マップの最後に配置されます。**class-default** クラスには **match any** が黙示的に含まれているので、他のトラフィック クラスに一致しないすべてのパケットが **class-default** に一致します。

	コマンド	目的
ステップ 5	**trust** [**cos** | **dscp** | **ip-precedence**]	CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼ステートを設定します。 （注）　このコマンドと **set** コマンドは、同じポリシー マップ内で相互に排他的になります。**trust** コマンドを入力する場合は、ステップ 6 へ進みます。 デフォルトでは、ポートは trusted ではありません。キーワードが指定されず、コマンドが入力されている場合、デフォルトは **dscp** です。 キーワードの意味は次のとおりです。 • **cos** : QoS は受信した CoS 値やデフォルトのポート CoS 値、および CoS/DSCP マップを使用して、DSCP 値を抽出します。 • **dscp** : QoS は入力パケットの DSCP 値を使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルト ポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 • **ip-precedence** : QoS は入力パケットの IP precedence 値および IP precedence/DSCP マップを使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルト ポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 詳細については、「CoS/DSCP マップの設定」（P.37-76）を参照してください。
ステップ 6	**set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*}	パケットに新しい値を設定することによって、IP トラフィックを分類します。 • **dscp** *new-dscp* には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *new-precedence* を指定する場合は、分類されたトラフィックに割り当てる新しい IP precedence 値を入力します。指定できる範囲は 0 ～ 7 です。

	コマンド	目的
ステップ 7	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]	分類したトラフィックにポリサーを定義します。 デフォルトでは、ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」（P.37-38）を参照してください。 • *rate-bps* には、平均トラフィック レートをビット/秒（bps）で指定します。指定できる範囲は 8000 ～ 10000000000 です。 • *burst-byte* には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ～ 1000000 です。 • （任意）レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、**exceed-action drop** キーワードを使用します。（ポリシング設定 DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」（P.37-78）を参照してください。
ステップ 8	**exit**	ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *interface-id*	ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 11	**service-policy input** *policy-map-name*	ポリシーマップ名を指定し、入力ポートに適用します。 サポートされるポリシー マップは、入力ポートに 1 つのみです。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]	エントリを確認します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除するには、**no class** *class-map-name* ポリシー マップ コンフィギュレーション コマンドを使用します。デフォルトの信頼できない状態に戻すには、**no trust** ポリシーマップ コンフィギュレーション コマンドを使用します。割り当てられた DSCP または IP precedence 値を削除するには、**no set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*} ポリシーマップ コンフィギュレーション コマンドを使用します。既存のポリサーを削除するには、**no police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}] ポリシーマップ コンフィギュレーション コマンドを使用します。ポリシー マップとポートの関連付けを解除するには、**no service-policy input** *policy-map-name* インターフェイス コンフィギュレーション コマンドを使用します。

次の例は、ポリシー マップを作成し、入力ポートに適用する方法を示しています。この設定では、IP 標準 ACL でネットワーク 10.1.0.0 からのトラフィックを許可します。この分類と一致するトラフィックの場合、着信パケットの DSCP 値は信頼されます。一致したトラフィックが平均トラフィック レート（48000bps）および標準バースト サイズ（8000 バイト）を超えた場合、（ポリシング設定 DSCP マップに基づいて）DSCP がマークダウンされて送信されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
```

```
Switch(config)# policy-map flow1t
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input flow1t
```

次に、2 つの permit ステートメントを指定してレイヤ 2 MAC ACL を作成し、入力ポートに適用する例を示します。最初の permit ステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。2 番めの permit ステートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、Ethertype が XNS-IDP のトラフィックだけが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-mac)# exit
Switch(config)# mac access-list extended maclist2
Switch(config-ext-mac)# permit 0001.0000.0003 0.0.0 0002.0000.0003 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0004 0.0.0 0002.0000.0004 0.0.0 aarp
Switch(config-ext-mac)# exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group maclist1
Switch(config-cmap)# exit
Switch(config)# policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set dscp 63
Switch(config-pmap-c)# exit
Switch(config-pmap)# class macclass2 maclist2
Switch(config-pmap-c)# set dscp 45
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

次に、IPv4 トラフィックと IPv6 トラフィックの両方に適用するクラス マップを作成する例を示します。

```
Switch(config)# ip access-list 101 permit ip any any
Switch(config)# ipv6 access-list ipv6-any permit ip any any
Switch(config)# Class-map cm-1
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-2
Switch(config-cmap)# match access-group name ipv6-any
Switch(config-cmap)# exit
Switch(config)# policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G0/1
Switch(config-if)# switch mode access
Switch(config-if)# service-policy input pm1
```

階層型ポリシー マップを使用した SVI のトラフィックの分類、ポリシング、およびマーキング

階層型ポリシー マップは SVI には設定できますが、他のタイプのインターフェイスには設定できません。階層型ポリシングは、VLAN レベルおよびインターフェイスレベル ポリシー マップを組み合わせて、単一ポリシー マップを作成します。

SVI では、VLAN レベルのポリシー マップが作用対象とするトラフィック クラスを指定します。アクションには、CoS、DSCP、IP precedence 値の信頼、またはトラフィック クラスの特定の DSCP、IP precedence 値の設定が含まれます。個々のポリサーで作用を受ける物理ポートを指定するには、インターフェイス レベルのポリシー マップを使用します。

Cisco IOS Release 12.2(52)SE 以降のリリースでは、IPv4 および IPv6 トラフィックをフィルタリングする階層型ポリシー マップを設定できます。

階層型ポリシー マップの設定を行うときは、次の注意事項に従ってください。

- 階層型ポリシー マップの設定を行う前に、ポリシー マップのインターフェイス レベルで指定する物理ポート上の VLAN ベース QoS をイネーブルにする必要があります。
- 入力ポートまたは SVI ごとに付加できるポリシー マップは、1 つだけです。
- 1 つのポリシー マップに、それぞれ異なる一致条件とアクションを指定した複数のクラス ステートメントを指定できます。
- SVI で受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。
- **mls qos map ip-prec-dscp** *dscp1...dscp8* グローバル コンフィギュレーション コマンドを使用して IP-precedence/DSCP マップを設定する場合、その設定は IP precedence 値を信頼するよう設定されている入力インターフェイス上のパケットにだけ影響を与えます。ポリシー マップでは、**set ip precedence** *new-precedence* ポリシーマップ クラス コンフィギュレーション コマンドを使用してパケット IP precedence 値に新規の値を設定すると、出力 DSCP 値は IP precedence/DSCP マップからは影響を受けません。出力 DSCP 値を入力値とは異なる値に設定する場合、**set dscp** *new-dscp* ポリシー マップ クラス コンフィギュレーション コマンドを使用します。
- **set ip dscp** コマンドを入力または使用すると、スイッチによってこのコマンドがスイッチ コンフィギュレーションの **set dscp** に変更されます。**set ip dscp** コマンドを入力すると、スイッチ コンフィギュレーションではこの設定は **set dscp** として表示されます。
- パケット IP precedence 値を変更するには、**set ip precedence** または **set precedence** ポリシー マップ クラス コンフィギュレーション コマンドを使用できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。
- VLAN ベース QoS がイネーブルになっている場合、階層型ポリシー マップは、以前に設定されたポートベース ポリシー マップに優先します。
- 階層型ポリシー マップが SVI に付加され、VLAN 内のすべてのトラフィックに影響を与えます。VLAN レベル ポリシー マップで指定されたアクションは、SVI に属するトラフィックに影響を与えます。ポート レベル ポリシー マップのポリシング アクションは、対象の物理インターフェイスの着信トラフィックに影響を与えます。
- トランク ポートの階層型ポリシー マップを設定する場合、VLAN の範囲が重複してはなりません。範囲が重複すると、ポリシー マップで指定されたアクションは、重複した VLAN 上の着信および送信トラフィックに影響を与えます。
- 集約ポリサーは、階層型ポリシー マップでサポートされていません。
- VLAN ベースの QoS がイネーブルになると、スイッチは VLAN マップなどの VLAN ベースの機能をサポートします。

- プライベート VLAN のプライマリ VLAN でだけ、デュアルレベル ポリシー マップを設定できます。
- VLAN ベースの QoS をイネーブルにして、階層型ポリシー マップをスイッチ スタックに設定すると、スタック設定の変更時に次に示すアクションが自動的に実行されます。
  - 新しいスタック マスターが選択されると、そのスタック マスターにより、スタック マスターの該当するすべてのインターフェイスでこれらの機能が再びイネーブルにされ、再設定されます。
  - スタック メンバーが追加されると、そのスタック マスターにより、スタック メンバーの該当するすべてのポートでこれらの機能が再びイネーブルにされ、再設定されます。
  - スイッチ スタックをマージすると、新しいスタック マスターにより、新しいスタックのスイッチでこれらの機能が再びイネーブルにされ、再設定されます。
  - スイッチ スタックが複数のスイッチ スタックに分割されると、各スイッチ スタックのスタック マスターにより、スタック マスターを含む、スタック メンバーのすべての該当するインターフェイスでこれらの機能が再びイネーブルにされ、再設定されます。
- **class class-default** ポリシーマップ コンフィギュレーション コマンドを使用してデフォルトのトラフィック クラスを設定すると、未分類のトラフィック（トラフィック クラスで指定された一致基準を満たさないトラフィック）は、デフォルトのトラフィック クラス（**class-default**）として処理されます。

ポリシー マップを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** [**match-all** | **match-any**] *class-map-name*	VLAN レベルのクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。クラス マップの作成については、「クラス マップを使用したトラフィックの分類」（P.37-55）を参照してください。 デフォルトでは、クラス マップは定義されていません。 • （任意）このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、**match-all** キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • （任意）このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、**match-any** キーワードを使用します。この場合は、1 つ以上の一致条件と一致する必要があります。 • *class-map-name* には、クラス マップ名を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 （注）　クラス マップごとにサポートされる **match** コマンドは 1 つだけのため、**match-all** でも **match-any** でもキーワードの機能は変わりません。**match-all** および **match-any** キーワードの使用に関する制限事項については、「名前付き標準および拡張 ACL の作成」（P.35-15）を参照してください。

	コマンド	目的
ステップ 3	**match** {**access-group** *acl-index-or-name* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}	トラフィックを分類するための一致条件を定義します。 デフォルトでは、一致条件は定義されていません。 クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。 • **access-group** *acl-index-or-name* には、ACL の番号または名前を指定します。 • **ip dscp** *dscp-list* には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *ip-precedence-list* には、着信パケットと照合する IP precedence 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。
ステップ 4	**match protocol** [*ip* | *ipv6*]	（任意）クラス マップを適用する IP プロトコルを指定します。 • IPv4 トラフィックを指定するには引数 *ip* を使用し、IPv6 トラフィックを指定するには *ipv6* を使用します。 • **match protocol** コマンドを使用する場合、**match-all** キーワードだけが最初のレベル クラス マップでサポートされます。 （注）　このコマンドは、デュアル IPv4/IPv6 SDM テンプレートが設定されている場合だけ使用できます。 **match protocol** コマンドは、**match ip dscp** または **match precedence** コマンドと使用できますが、**match access-group** コマンドとは使用できません。 **match protocol** コマンドの詳細については、『*Cisco IOS Quality of Service Solutions Command Reference*』を参照してください。
ステップ 5	**exit**	クラスマップ コンフィギュレーション モードに戻ります。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 7	**class-map** [**match-all** | **match-any**] *class-map-name*	インターフェイス レベルのクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 • （任意）このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、**match-all** キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • （任意）このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、**match-any** キーワードを使用します。この場合は、1 つ以上の一致条件と一致する必要があります。 • *class-map-name* には、クラス マップ名を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 **（注）** クラス マップごとにサポートされる **match** コマンドは 1 つだけのため、**match-all** でも **match-any** でもキーワードの機能は変わりません。**match-all** および **match-any** キーワードの使用に関する制限事項については、「名前付き標準および拡張 ACL の作成」（P.35-15）を参照してください。
ステップ 8	**match input-interface** *interface-id-list*	インターフェイス レベルのクラス マップを実行する物理ポートを指定します。次の方法で、最大 6 つのポートを指定できます。 • 単一のポート（1 つのエントリとしてカウントされます） • スペースで区切られたポートのリスト（各ポートが 1 つのエントリとしてカウントされます） • ハイフンで区切られたポートの範囲（2 つのエントリとしてカウントされます） このコマンドは、子レベルのポリシー マップでのみ使用でき、子レベルのポリシー マップ内での唯一の一致条件である必要があります。
ステップ 9	**exit**	クラスマップ コンフィギュレーション モードに戻ります。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**policy-map** *policy-map-name*	ポリシー マップ名を入力してインターフェイス レベルのポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されておらず、ポリサーも実行されていません。
ステップ 12	**class-map** *class-map-name*	インターフェイス レベルのトラフィック分類を定義し、ポリシーマップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップのクラス マップは定義されていません。 すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。

	コマンド	目的
ステップ 13	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]	分類したトラフィックにそれぞれポリサーを定義します。 デフォルトでは、ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」（P.37-38）を参照してください。 • *rate-bps* には、平均トラフィック レートをビット/秒（bps）で指定します。指定できる範囲は 8000 ～ 10000000000 です。 • *burst-byte* には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ～ 1000000 です。 • （任意）レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、**exceed-action drop** キーワードを使用します。（ポリシング設定 DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」（P.37-78）を参照してください。
ステップ 14	**exit**	ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 15	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**policy-map** *policy-map-name*	ポリシー マップ名を入力することによって VLAN レベルのポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されていません。 ポリシー マップのデフォルト動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。
ステップ 17	**class** [*class-map-name* | **class-default**]	VLAN レベルのトラフィック分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップのクラス マップは定義されていません。 すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。 **class-default** トラフィック クラスは、事前に定義されており、任意のポリシーに追加できます。このクラスは、常にポリシー マップの最後に配置されます。**class-default** クラスには **match any** が黙示的に含まれているので、他のトラフィック クラスに一致しないすべてのパケットが **class-default** に一致します。

	コマンド	目的
ステップ 18	**trust** [**cos** | **dscp** | **ip-precedence**]	CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼ステートを設定します。 （注）　このコマンドと **set** コマンドは、同じポリシー マップ内で相互に排他的になります。**trust** コマンドを入力する場合は、ステップ 18 を省略してください。 デフォルトでは、ポートは trusted ではありません。キーワードが指定されず、コマンドが入力されている場合、デフォルトは **dscp** です。 キーワードの意味は次のとおりです。 • **cos** : QoS は受信した CoS 値やデフォルトのポート CoS 値、および CoS/DSCP マップを使用して、DSCP 値を抽出します。 • **dscp** : QoS は入力パケットの DSCP 値を使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルト ポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 • **ip-precedence** : QoS は入力パケットの IP precedence 値および IP precedence/DSCP マップを使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルト ポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 詳細については、「CoS/DSCP マップの設定」（P.37-76）を参照してください。
ステップ 19	**set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*}	パケットに新しい値を設定することによって、IP トラフィックを分類します。 • **dscp** *new-dscp* には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *new-precedence* を指定する場合は、分類されたトラフィックに割り当てる新しい IP precedence 値を入力します。指定できる範囲は 0 ～ 7 です。
ステップ 20	**service-policy** *policy-map-name*	インターフェイスレベルのポリシーマップ名を指定し（ステップ 10 を参照）、VLAN レベルのポリシー マップと連動させます。 VLAN レベル ポリシー マップが 2 つ以上のクラスを指定している場合、各クラスで異なる **service-policy** *policy-map-name* コマンドを使用できます。
ステップ 21	**exit**	ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 22	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 23	**interface** *interface-id*	階層型のポリシー マップを適用する SVI を指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 24	**service-policy input** *policy-map-name*	VLAN レベルのポリシーマップ名を指定し、SVI にそれを適用します。前のステップとこのコマンドを使用して、他の SVI にポリシーマップを適用します。 階層型 VLAN レベル ポリシー マップに 2 つ以上のインターフェイス レベル ポリシー マップがある場合、すべてのクラス マップが、**service-policy** *policy-map-name* コマンドで指定された同じ VLAN レベル ポリシー マップに設定されている必要があります。
ステップ 25	**end**	特権 EXEC モードに戻ります。
ステップ 26	**show policy-map** [*policy-map-name* [**class** *class-map-name*]] または **show mls qos vlan-based**	エントリを確認します。
ステップ 27	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除するには、**no class** *class-map-name* ポリシー マップ コンフィギュレーション コマンドを使用します。

ポリシー マップで信頼できない状態に戻すには、**no trust** ポリシーマップ コンフィギュレーション コマンドを使用します。割り当てられた DSCP または IP precedence 値を削除するには、**no set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*} ポリシーマップ コンフィギュレーション コマンドを使用します。

インターフェイス レベルのポリシー マップの既存のポリサーを削除するには、**no police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}] ポリシー マップ コンフィギュレーション コマンドを使用します。デュアルレベル ポリシー マップとポートの関連付けを解除するには、**no service-policy input** *policy-map-name* インターフェイス コンフィギュレーション コマンドを使用します。

次に、階層型ポリシー マップを作成する例を示します。

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# access-list 101 permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access 101
Switch(config-cmap)# exit
Switch(config)# exit
Switch#
Switch#
```

次に、新しいマップを SVI に適用する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map cm-interface-1
Switch(config-cmap)# match input gigabitethernet3/0/1 - gigabitethernet3/0/2
Switch(config-cmap)# exit
Switch(config)# policy-map port-plcmap
Switch(config-pmap)# class cm-interface-1
Switch(config-pmap-c)# police 900000 9000 exc policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map vlan-plcmap
Switch(config-pmap)# class cm-1
```

```
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap)# exit
Switch(config-pmap)# class cm-3
Switch(config-pmap-c)# set dscp 20
Switch(config-pmap-c)# service-policy port-plcmap-2
Switch(config-pmap)# exit
Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# trust dscp
Switch(config-pmap)# exit
Switch(config)# interface vlan 10
Switch(config-if)# service input vlan-plcmap
Switch(config-if)# exit
Switch(config)# exit
Switch#
```

次に、IP DSCP および IPv6 と照合するクラス マップを設定する例を示します。

```
Switch(config)# class-map cm-1
Switch(config-cmap)# match ip dscp 10
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)# class-map cm-2
Switch(config-cmap)# match ip dscp 20
Switch(config-cmap)# match protocol ip
Switch(config-cmap)# exit
Switch(config)# policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G1/0/1
Switch(config-if)# service-policy input pm1
```

次の例では、ポリシー マップにデフォルトのトラフィック クラスを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# class-map cm-3
Switch(config-cmap)# match ip dscp 30
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)# class-map cm-4
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# match protocol ip
Switch(config-cmap)# exit
Switch(config)# policy-map pm3
Switch(config-pmap)# class class-default
Switch(config-pmap)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-3
Switch(config-pmap-c) set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# trust cos
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

この例では、class-default が最初に設定されていても、デフォルトのトラフィック クラスは、自動的に policy-map pm3 の最後に配置されることを示します。

```
Switch# show policy-map pm3
  Policy Map pm3
    Class cm-3
      set dscp 4
    Class cm-4
      trust cos
    Class class-default
      police 8000 80000 exceed-action drop
Switch#
```

集約ポリサーを使用したトラフィックの分類、ポリシング、およびマーキング

集約ポリサーを使用すると、同じポリシー マップ内の複数のトラフィック クラスで共有されるポリサーを作成できます。ただし、集約ポリサーを複数の異なるポリシー マップまたはポートにわたって使用することはできません。

集約ポリサーは、物理ポートの非階層型ポリシー マップでだけ設定できます。

集約ポリサーを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos aggregate-policer** *aggregate-policer-name rate-bps burst-byte* **exceed-action** {**drop** | **policed-dscp-transmit**}	同じポリシー マップ内の複数のトラフィック クラスに適用できるポリサー パラメータを定義します。 デフォルトでは、集約ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」（P.37-38）を参照してください。 • *aggregate-policer-name* には、集約ポリサーの名前を指定します。 • *rate-bps* には、平均トラフィック レートをビット/秒（bps）で指定します。指定できる範囲は 8000 ～ 10000000000 です。 • *burst-byte* には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ～ 1000000 です。 • レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、**exceed-action drop** キーワードを使用します。（ポリシング設定 DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」（P.37-78）を参照してください。
ステップ 3	**class-map** [**match-all** | **match-any**] *class-map-name*	必要に応じて、トラフィックを分類するクラス マップを作成します。詳細については、「クラス マップを使用したトラフィックの分類」（P.37-55）および「名前付き標準および拡張 ACL の作成」（P.35-15）を参照してください。

	コマンド	目的
ステップ 4	**policy-map** *policy-map-name*	ポリシー マップ名を入力することによってポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。 詳細については、「ポリシー マップを使用した物理ポートのトラフィックの分類、ポリシング、およびマーキング」（P.37-61）を参照してください。
ステップ 5	**class** [*class-map-name* | **class-default**]	トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 詳細については、「ポリシー マップを使用した物理ポートのトラフィックの分類、ポリシング、およびマーキング」（P.37-61）を参照してください。
ステップ 6	**police aggregate** *aggregate-policer-name*	同じポリシー マップ内の複数のクラスに集約ポリサーを適用します。 *aggregate-policer-name* には、ステップ 2 で指定した名前を入力します。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *interface-id*	ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 9	**service-policy input** *policy-map-name*	ポリシーマップ名を指定し、入力ポートに適用します。 サポートされるポリシー マップは、入力ポートに 1 つのみです。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show mls qos aggregate-policer** [*aggregate-policer-name*]	エントリを確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

指定した集約ポリサーをポリシー マップから削除するには、**no police aggregate** *aggregate-policer-name* ポリシーマップ コンフィギュレーション モードを使用します。集約ポリサーおよびそのパラメータを削除するには、**no mls qos aggregate-policer** *aggregate-policer-name* グローバル コンフィギュレーション コマンドを使用します。

次に、集約ポリサーを作成して、ポリシー マップ内の複数のクラスに結合する例を示します。この設定では、IP ACL はネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィックを許可します。ネットワーク 10.1.0.0 からのトラフィックの場合、着信パケットの DSCP は信頼されます。ホスト 11.3.1.1 から着信するトラフィックの場合、パケットの DSCP は 56 に変更されます。ネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィック レートには、ポリシングが設定されます。トラフィックが平均レート（48000 b/s）および標準バースト サイズ（8000 バイト）を超えた場合、（ポリシング設定 DSCP マップに基づいて）DSCP がマークダウンされて転送されます。このポリシー マップが入力ポートに付加されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# access-list 2 permit 11.3.1.1
Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action
policed-dscp-transmit
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map ipclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
```

```
Switch(config)# policy-map aggflow1
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class ipclass2
Switch(config-pmap-c)# set dscp 56
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input aggflow1
Switch(config-if)# exit
```

DSCP マップの設定

ここでは、次の設定情報について説明します。

- 「CoS/DSCP マップの設定」（P.37-76）（任意）
- 「IP precedence/DSCP マップの設定」（P.37-77）（任意）
- 「ポリシング済み DSCP マップの設定」（P.37-78）（任意、マップのヌル設定が不適切な場合以外）
- 「DSCP/CoS マップの設定」（P.37-79）（任意）
- 「DSCP/DSCP 変換マップの設定」（P.37-80）（任意、マップのヌル設定が不適切な場合以外）

DSCP/DSCP 変換マップを除くすべてのマップはグローバルに定義され、すべてのポートに適用されます。

CoS/DSCP マップの設定

着信パケットの CoS 値を、トラフィックのプライオリティを表すために QoS で内部的に使用される DSCP 値にマッピングするには、CoS/DSCP マップを使用します。

表 37-12 に、デフォルトの CoS/DSCP マップを示します。

表 37-12　デフォルトの CoS/DSCP マップ

CoS 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

CoS/DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map cos-dscp** *dscp1...dscp8*	CoS/DSCP マップを変更します。 *dscp1...dscp8* には、CoS 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ～ 63 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps cos-dscp**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、**no mls qos cos-dscp** グローバル コンフィギュレーション コマンドを使用します。

次に、CoS/DSCP マップを変更して表示する例を示します。

```
Switch(config)# mls qos map cos-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps cos-dscp

Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
      --------------------------------
       dscp:   10 15 20 25 30 35 40 45
```

IP precedence/DSCP マップの設定

着信パケットの IP precedence 値を、トラフィックのプライオリティを表すために QoS で内部的に使用される DSCP 値にマッピングするには、IP precedence/DSCP マップを使用します。

表 37-13 に、デフォルトの IP precedence/DSCP マップを示します。

表 37-13　デフォルトの IP Precedence/DSCP マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

IP precedence/DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map ip-prec-dscp** *dscp1...dscp8*	IP precedence/DSCP マップを変更します。 *dscp1...dscp8* には、IP precedence 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ～ 63 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps ip-prec-dscp**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、**no mls qos ip-prec-dscp** グローバル コンフィギュレーション コマンドを使用します。

次に、IP precedence/DSCP マップを変更して表示する例を示します。

```
Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps ip-prec-dscp

IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   10 15 20 25 30 35 40 45
```

ポリシング済み DSCP マップの設定

ポリシングおよびマーキング アクションによって得られる新しい値に DSCP 値をマークダウンするには、ポリシング設定 DSCP マップを使用します。

デフォルトのポリシング設定 DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌルマップです。

ポリシング済み DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map policed-dscp** *dscp-list* **to** *mark-down-dscp*	ポリシング済み DSCP マップを変更します。 • *dscp-list* には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *mark-down-dscp* には、対応するポリシング設定（マークダウンされた）DSCP 値を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps policed-dscp**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、**no mls qos policed-dscp** グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 50 ～ 57 を、マークダウンされる DSCP 値 0 にマッピングする例を示します。

```
Switch(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0
Switch(config)# end
Switch# show mls qos maps policed-dscp
Policed-dscp map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    00 00 00 00 00 00 00 00 58 59
      6 :    60 61 62 63
```

（注）　このポリシング済み DSCP マップでは、マークダウンされる DSCP 値が表形式で示されています。d1 列では元の DSCP の最上位桁、d2 行では元の DSCP の最下位桁を指定します。d1 と d2 の交点にある値が、マークダウンされる値です。たとえば、元の DSCP 値が 53 の場合、マークダウンされる DSCP 値は 0 です。

DSCP/CoS マップの設定

4 つの出力キューセットの 1 つを選択するために使用される CoS 値を生成するには、DSCP/CoS マップを使用します。

表 37-14 に、デフォルトの DSCP/CoS マップを示します。

表 37-14　デフォルトの DSCP/CoS マップ

DSCP 値	CoS 値
0 ～ 7	0
8 ～ 15	1
16 ～ 23	2
24 ～ 31	3
32 ～ 39	4
40 ～ 47	5
48 ～ 55	6
56 ～ 63	7

これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

DSCP/CoS マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-cos** *dscp-list* **to** *cos*	DSCP/CoS マップを変更します。 • *dscp-list* には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *cos* には、DSCP 値と対応する CoS 値を入力します。 DSCP の範囲は 0 ～ 63、CoS の範囲は 0 ～ 7 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps dscp-to-cos**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、**no mls qos dscp-cos** グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 値 0、8、16、24、32、40、48、および 50 を CoS 値 0 にマッピングして、マップを表示する例を示します。

```
Switch(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 50 to 0
Switch(config)# end
Switch# show mls qos maps dscp-cos
Dscp-cos map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------------
      0 :    00 00 00 00 00 00 00 00 00 01
      1 :    01 01 01 01 01 01 00 02 02 02
      2 :    02 02 02 02 00 03 03 03 03 03
      3 :    03 03 00 04 04 04 04 04 04 04
      4 :    00 05 05 05 05 05 05 05 00 06
      5 :    00 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

（注）上記の DSCP/CoS マップでは、CoS 値が表形式で示されています。d1 列では DSCP の最上位桁、d2 行では DSCP の最下位桁を指定します。d1 と d2 の交点にある値が CoS 値です。たとえば、この DSCP/CoS マップでは、DSCP 値が 08 の場合、対応する CoS 値は 0 です。

DSCP/DSCP 変換マップの設定

2 つの QoS ドメインで異なる DSCP 定義が使用されている場合は、一方のドメインの一連の DSCP 値を変換して、もう一方のドメインの定義に一致させる DSCP/DSCP 変換マップを使用します。DSCP/DSCP 変換マップは、QoS 管理ドメインの境界にある受信ポート適用します（入力変換）。

入力変換により、パケットの DSCP 値が新しい DSCP 値で上書きされ、QoS はこの新しい値を使用してパケットを処理します。スイッチは、新しい DSCP 値とともにそのパケットをポートへ送出します。

1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

DSCP/DSCP 変換マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*	DSCP/DSCP 変換マップを変更します。 • *dscp-mutation-name* には、変換マップ名を入力します。新しい名前を指定することにより、複数のマップを作成できます。 • *in-dscp* には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *out-dscp* には、1 つの DSCP 値を入力します。 DSCP の範囲は 0 ～ 63 です。
ステップ 3	**interface** *interface-id*	マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 4	**mls qos trust dscp**	DSCP trusted ポートとして入力ポートを設定します。デフォルトでは、ポートは trusted ではありません。
ステップ 5	**mls qos dscp-mutation** *dscp-mutation-name*	指定された DSCP trusted 入力ポートにマップを適用します。 *dscp-mutation-name* には、ステップ 2 で指定した変換マップ名を入力します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show mls qos maps dscp-mutation**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、**no mls qos dscp-mutation** *dscp-mutation-name* グローバル コンフィギュレーション コマンドを使用します。

次の例では、DSCP/DSCP 変換マップを定義する方法を示します。明示的に設定されていないすべてのエントリは変更されません（ヌル マップで指定された値のままです）。

```
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation mutation1
Switch(config-if)# end
Switch# show mls qos maps dscp-mutation mutation1
Dscp-dscp mutation map:
   mutation1:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------------
      0 :    00 00 00 00 00 00 00 00 10 10
      1 :    10 10 10 10 14 15 16 17 18 19
      2 :    20 20 20 23 24 25 26 27 28 29
      3 :    30 30 30 30 30 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
```

（注）　上記の DSCP/DSCP 変換マップでは、変換される値が表形式で示されています。d1 列では元の DSCP の最上位桁、d2 行では元の DSCP の最下位桁を指定します。d1 と d2 の交点の値が、変換される値です。たとえば、DSCP 値が 12 の場合、対応する変換される値は 10 です。

入力キューの特性の設定

ネットワークおよび QoS ソリューションの複雑さに応じて、次に示す作業をすべて実行しなければならない場合があります。次の特性を決定する必要があります。

- 各キューに（DSCP 値または CoS 値によって）割り当てるパケット
- 各キューに適用されるドロップ パーセンテージしきい値、および各しきい値にマッピングされる CoS または DSCP 値
- 各キュー間に割り当てられる空きバッファ スペースの量
- 各キュー間に割り当てられる使用可能な帯域幅の量
- ハイ プライオリティを設定する必要があるトラフィック（音声など）の有無

ここでは、次の設定情報について説明します。

- 「入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定」（P.37-83）（任意）
- 「入力キュー間のバッファ スペースの割り当て」（P.37-84）（任意）
- 「入力キュー間の帯域幅の割り当て」（P.37-85）（任意）
- 「入力プライオリティ キューの設定」（P.37-85）（任意）

入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定

トラフィックにプライオリティを設定するには、特定の DSCP または CoS を持つパケットを特定のキューに格納し、より低いプライオリティを持つパケットがドロップされるようにキューのしきい値を調整します。

DSCP または CoS 値を入力キューにマッピングして、WTD しきい値を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input dscp-map queue** *queue-id* **threshold** *threshold-id dscp1...dscp8* または **mls qos srr-queue input cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8*	DSCP または CoS 値を入力キューおよびしきい値 ID にマッピングします。 デフォルトでは、DSCP 値 0 ～ 39 および 48 ～ 63 はキュー 1 およびしきい値 1 にマッピングされます。DSCP 値 40 ～ 47 はキュー 2 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 ～ 4、6、および 7 はキュー 1 およびしきい値 1 にマッピングされます。CoS 値 5 はキュー 2 およびしきい値 1 にマッピングされます。 • *queue-id* で指定できる範囲は 1 ～ 2 です。 • *threshold-id* で指定できる範囲は 1 ～ 3 です。しきい値 3 のドロップしきい値（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。 • *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ～ 63 です。 • *cos1...cos8* には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。
ステップ 3	**mls qos srr-queue input threshold** *queue-id threshold-percentage1 threshold-percentage2*	入力キューに 2 つの WTD しきい値の割合（しきい値 1 および 2 用）を割り当てます。デフォルトでは、両方のしきい値が 100% に設定されています。 • *queue-id* で指定できる範囲は 1 ～ 2 です。 • *threshold-percentage1 threshold-percentage2* の範囲は、1 ～ 100 です。各値はスペースで区切ります。 各しきい値は、キューに割り当てられたキュー記述子の総数に対する割合です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos maps**	設定を確認します。 DSCP 入力キューしきい値マップは、表形式で表示されます。d1 列では DSCP 値の最上位桁、d2 行では DSCP 値の最下位桁を指定します。d1 および d2 値の交点がキュー ID およびしきい値 ID です。たとえば、キュー 2 およびしきい値 1（02-01）のようになります。 CoS 入力キューしきい値マップでは、先頭行に CoS 値、2 番めの行に対応するキュー ID およびしきい値 ID が示されます。たとえば、キュー 2 およびしきい値 2（2-2）のようになります。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの CoS 入力キューしきい値マップまたはデフォルトの DSCP 入力キューしきい値マップに戻すには、**no mls qos srr-queue input cos-map**、または **no mls qos srr-queue input dscp-map** グローバル コンフィギュレーション コマンドを使用します。デフォルトの WTD しきい値の割合に戻すには、**no mls qos srr-queue input threshold** *queue-id* グローバル コンフィギュレーション コマンドを使用します。

次の例では、DSCP 値 0 ～ 6 を、入力キュー 1 とドロップしきい値 50% のしきい値 1 にマッピングする方法を示します。DSCP 値 20 と 26 は、入力キュー 1 とドロップしきい値 70% のしきい値 2 にマッピングします。

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

この例では、50% の WTD しきい値が DSCP 値（0 ～ 6）に割り当てられており、70% の WTD しきい値が割り当てられた DSCP 値（20 ～ 26）よりも先にドロップされます。

入力キュー間のバッファ スペースの割り当て

2 つのキュー間で入力バッファを分割する比率を定義します（スペース量を割り当てます）。バッファ割り当てと帯域幅割り当てにより、パケットがドロップされる前にバッファに格納できるデータ量が制御されます。

入力キュー間にバッファを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input buffers** *percentage1 percentage2*	入力キュー間にバッファを割り当てます。 デフォルトでは、バッファの 90% がキュー 1 に、残りの 10% がキュー 2 に割り当てられます。 *percentage1 percentage2* の範囲は、0 ～ 100 です。各値はスペースで区切ります。 キューがバースト性のある着信トラフィックを処理できるようにバッファを割り当てる必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos interface buffer** または **show mls qos input-queue**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no mls qos srr-queue input buffers** グローバル コンフィギュレーション コマンドを使用します。

次の例では、入力キュー 1 にバッファ スペースの 60% を、入力キュー 2 にバッファ スペースの 40% を割り当てる方法を示します。

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

入力キュー間の帯域幅の割り当て

入力キュー間に割り当てられる使用可能な帯域幅の量を指定する必要があります。重みの比率は、SRR スケジューラがパケットを各キューから送り出す頻度の比率です。帯域幅割り当てとバッファ割り当てにより、パケットがドロップされる前にバッファに格納できるデータ量を制御できます。入力キューで SRR が動作するのは、共有モードの場合だけです。

入力キュー間に帯域幅を割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input bandwidth** *weight1 weight2*	入力キューに共有ラウンド ロビン重みを割り当てます。 *weight1* と *weight2* のデフォルト設定は 4 です（帯域幅の 1/2 が 2 つのキューで等しく共有されます）。 *weight1* と *weight2* の範囲は、1 ～ 100 です。各値はスペースで区切ります。 SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に、SRR は **mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。詳細については、「入力プライオリティ キューの設定」（P.37-85）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos interface queueing** または **show mls qos input-queue**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no mls qos srr-queue input bandwidth** グローバル コンフィギュレーション コマンドを使用します。

次に、キューに入力帯域幅を割り当てる例を示します。プライオリティ キューイングはディセーブルです。割り当てられる共有帯域幅の比率は、キュー 1 が 25/（25+75）、キュー 2 が 75/（25+75）です。

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

入力プライオリティ キューの設定

プライオリティ キューは、優先して進める必要があるトラフィックにのみ使用してください（遅延とジッタを最小限にとどめる必要のある音声トラフィックなど）。

プライオリティ キューは、オーバーサブスクライブ リングに激しいネットワーク トラフィックが発生している状況で（バックプレーンが伝達できるトラフィックよりも多くのトラフィックが発生し、キューがいっぱいになって、フレームがドロップされている場合）、遅延およびジッタを軽減するように帯域幅の一部が保証されています。

SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に、SRR は **mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。

プライオリティ キューを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight*	キューをプライオリティ キューとして割り当て、スタックまたは内部リングが輻輳している場合にリングの帯域幅を保証します。 デフォルトのプライオリティ キューはキュー 2 です。このキューには帯域幅の 10% が割り当てられています。 • *queue-id* で指定できる範囲は 1 ～ 2 です。 • **bandwidth** *weight* には、スタックまたは内部リングの帯域幅に対する割合を割り当てます。指定できる範囲は 0 ～ 40 です。値が大きい場合はリング全体に影響が及び、スイッチまたはスタックのパフォーマンスが低下することがあるため、保証できる帯域幅は制限されています。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos interface queueing** または **show mls qos input-queue**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no mls qos srr-queue input priority-queue** *queue-id* グローバル コンフィギュレーション コマンドを使用します。プライオリティ キューイングをディセーブルにするには、帯域幅の重みを 0 に設定します。たとえば、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth 0** を入力します。

次に、キューに入力帯域幅を割り当てる例を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 および 2 に割り当てられている帯域幅比率は 4/（4+4）です。SRR は最初、設定された 10% の帯域幅をキュー 1（プライオリティ キュー）にサービスします。そのあと、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

出力キューの特性の設定

ネットワークおよび QoS ソリューションの複雑さに応じて、次に示す作業をすべて実行しなければならない場合があります。次の特性を決定する必要があります。

- DSCP 値または CoS 値によって各キューおよびしきい値 ID にマッピングされるパケット
- キューセット（ポートごとの 4 つの出力キュー）に適用されるドロップ パーセンテージしきい値、およびトラフィック タイプに必要なメモリの確保量および最大メモリ
- キュー セットに割り当てる固定バッファ スペースの量

- ポートの帯域幅に関するレート制限の必要性
- 出力キューの処理頻度、および使用する技術（シェーピング、共有、または両方）

ここでは、次の設定情報について説明します。

- 「設定時の注意事項」（P.37-87）
- 「出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定」（P.37-87）（任意）
- 「出力キューおよびしきい値 ID への DSCP または CoS 値のマッピング」（P.37-89）（任意）
- 「出力キューの SRR シェーピング重みの設定」（P.37-91）（任意）
- 「出力キューでの SRR 共有重みの設定」（P.37-92）（任意）
- 「出力緊急キューの設定」（P.37-93）（任意）
- 「出力インターフェイスの帯域幅の制限」（P.37-93）（任意）

設定時の注意事項

緊急キューがイネーブルにされているとき、または SRR の重みに基づいて出力キューのサービスが提供されるときには、次の注意事項に従ってください。

- 出力緊急キューがイネーブルにされている場合は、キュー 1 に対して SRR のシェーピングおよび共有された重みが無効にされます。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングおよび共有された重みが設定されている場合は、キュー 1 に対して shaped モードは shared モードを無効にし、SRR はこのキューに shaped モードでサービスを提供します。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングされた重みが設定されていない場合は、SRR はキューに対して shared モードでサービスを提供します。

出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定

バッファのアベイラビリティの保証、WTD の設定、およびキューセットの最大割り当ての設定を行うには、**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* グローバル コンフィギュレーション コマンド を使用します。

各しきい値はキューに割り当てられたメモリの割合です。パーセンテージを指定するには、**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4* グローバル コンフィギュレーション コマンドを使用します。キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。

（注）　出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合のみ、設定を変更してください。

キューセットのメモリ割り当ておよびドロップしきい値を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4*	キューセットにバッファを割り当てます。 デフォルトでは、すべての割り当て値は 4 つのキューに均等にマッピングされます（25、25、25、25）。各キューがバッファ スペースの 1/4 を持ちます。 • *qset-id* には、キューセットの ID を入力します。指定できる範囲は 1 ～ 2 です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。 • *allocation1 ... allocation4* には、キューセットの各キューに 1 つずつ、合計 4 つの割合を指定します。*allocation1*、*allocation3*、および *allocation4* の場合、指定できる範囲は 0 ～ 99 です。*allocation2* の場合、指定できる範囲は 1 ～ 100 です（CPU バッファを含む）。 トラフィックの重要度に応じてバッファを割り当てます。たとえば、最高プライオリティのトラフィックを持つキューには多くの割合のバッファを与えます。
ステップ 3	**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold*	WTD を設定し、バッファのアベイラビリティを保証し、キューセット（ポートごとに 4 つの出力キュー）の最大メモリ割り当てを設定します。 デフォルトでは、キュー 1、3、および 4 の WTD は 100% に設定されています。キュー 2 の WTD は 200% に設定されています。キュー 1、2、3、および 4 の専用は 50% に設定されています。すべてのキューの最大は 400% に設定されています。 • *qset-id* には、ステップ 2 で指定したキューセットの ID を入力します。指定できる範囲は 1 ～ 2 です。 • *queue-id* には、コマンドの実行対象となるキューセット内の特定のキューを入力します。指定できる範囲は 1 ～ 4 です。 • *drop-threshold1 drop-threshold2* には、キューの割り当てメモリの割合として表される 2 つの WTD を指定します。指定できる範囲は 1 ～ 3200% です。 • *reserved-threshold* には、割り当てメモリの割合として表されるキューに保証（確保）されるメモリ サイズを入力します。指定できる範囲は 1 ～ 100% です。 • *maximum-threshold* には、フル状態のキューが、予約量を超えるバッファを取得できるようにします。この値は、共通プールが空でない場合に、パケットがドロップされるまでキューが使用できるメモリの最大値です。指定できる範囲は 1 ～ 3200% です。
ステップ 4	**interface** *interface-id*	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**queue-set** *qset-id*	キューセットにポートをマッピングします。 *qset-id* には、ステップ 2 で指定したキューセットの ID を入力します。指定できる範囲は 1 ～ 2 です。デフォルトは 1 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show mls qos interface** [*interface-id*] **buffers**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no mls qos queue-set output** *qset-id* **buffers** グローバル コンフィギュレーション コマンドを使用します。デフォルトの WTD の割合に戻すには、**no mls qos queue-set output** *qset-id* **threshold** [*queue-id*] グローバル コンフィギュレーション コマンドを使用します。

次の例では、ポートをキューセット 2 にマッピングする方法を示します。出力キュー 1 にバッファ スペースの 40% を、出力キュー 2、3、および 4 にはそれぞれ 20% ずつ割り当てます。キュー 2 のドロップしきい値を割り当てられたメモリの 40% と 60% に設定し、割り当てられたメモリの 100% を保証（予約）して、このキューがパケットをドロップせずに保持可能な最大メモリを 200% に設定します。

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# queue-set 2
```

出力キューおよびしきい値 ID への DSCP または CoS 値のマッピング

トラフィックにプライオリティを設定するには、特定の DSCP または CoS を持つパケットを特定のキューに格納し、より低いプライオリティを持つパケットがドロップされるようにキューのしきい値を調整します。

（注）　出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合のみ、設定を変更してください。

DSCP または CoS 値を出力キューおよび ID にマッピングするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue output dscp-map queue** *queue-id* **threshold** *threshold-id dscp1...dscp8* または **mls qos srr-queue output cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8*	DSCP または CoS 値を出力キューおよびしきい値 ID にマッピングします。 デフォルトでは、DSCP 値 0 ～ 15 はキュー 2 およびしきい値 1 にマッピングされます。DSCP 値 16 ～ 31 はキュー 3 およびしきい値 1 にマッピングされます。DSCP 値 32 ～ 39 および 48 ～ 63 はキュー 4 およびしきい値 1 にマッピングされます。DSCP 値 40 ～ 47 はキュー 1 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 および 1 はキュー 2 およびしきい値 1 にマッピングされます。CoS 値 2 および 3 はキュー 3 およびしきい値 1 にマッピングされます。CoS 値 4、6、および 7 はキュー 4 およびしきい値 1 にマッピングされます。CoS 値 5 はキュー 1 およびしきい値 1 にマッピングされます。 • *queue-id* で指定できる範囲は 1 ～ 4 です。 • *threshold-id* で指定できる範囲は 1 ～ 3 です。しきい値 3 のドロップしきい値（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。 • *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ～ 63 です。 • *cos1...cos8* には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps**	設定を確認します。 DSCP 出力キューしきい値マップは、表形式で表示されます。d1 列では DSCP 値の最上位桁、d2 行では DSCP 値の最下位桁を指定します。d1 および d2 値の交点がキュー ID およびしきい値 ID です。たとえば、キュー 2 およびしきい値 1（02-01）のようになります。 CoS 出力キューしきい値マップでは、先頭行に CoS 値、2 番めの行に対応するキュー ID およびしきい値 ID が示されます。たとえば、キュー 2 およびしきい値 2（2-2）のようになります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの DSCP 出力キューしきい値マップまたはデフォルトの CoS 出力キューしきい値マップに戻すには、**no mls qos srr-queue output dscp-map** または **no mls qos srr-queue output cos-map** グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 値 10 および 11 を出力キュー 1 およびしきい値 2 にマッピングする例を示します。

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 10 11
```

出力キューの SRR シェーピング重みの設定

各キューに割り当てる使用可能な帯域幅の比率を指定することができます。重みの比率は、SRR スケジューラがパケットを各キューから送り出す頻度の比率です。

出力キューには、シェーピング重み、共有重み、またはその両方を設定できます。バースト性のあるトラフィックをスムーズにする、または長期にわたって出力をスムーズにする場合に、シェーピングを使用します。シェーピング重みについては、「SRR のシェーピングおよび共有」（P.37-15）を参照してください。共有重みについては、「出力キューでの SRR 共有重みの設定」（P.37-92）を参照してください。

ポートにマッピングされた 4 つの出力キューにシェーピング重みを割り当てて、帯域幅のシェーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**srr-queue bandwidth shape** *weight1 weight2 weight3 weight4*	出力キューに SRR 重みを割り当てます。 デフォルトでは、weight1 は 25、weight2、weight3、および weight4 は 0 に設定されています。これらのキューは共有モードです。 *weight1 weight2 weight3 weight4* には、シェーピングされるポートの割合を制御する重みを入力します。このキューのシェーピング帯域幅は、インバース比率（1/*weight*）によって制御されます。各値はスペースで区切ります。指定できる範囲は 0 ～ 65535 です。 重み 0 を設定した場合は、対応するキューが共有モードで動作します。**srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。シェーピングおよび共有の両方に対して同じキューセットのキューを設定した場合は、必ず番号が最も小さいキューにシェーピングを設定してください。 シェーピング モードは、共有モードを無効にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** *interface-id* **queueing**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドを使用します。

次に、キュー 1 で帯域幅のシェーピングを設定する例を示します。キュー 2、3、4 の重み比が 0 に設定されているので、キューは共有モードで動作します。キュー 1 の帯域幅の重みは 1/8、12.5% です。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
```

出力キューでの SRR 共有重みの設定

共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、特定のキューが空であり、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有ができます。共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関係ありません。

（注）出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合のみ、設定を変更してください。

ポートにマッピングされた 4 つの出力キューに共有重みを割り当てて、帯域幅のシェーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**srr-queue bandwidth share** *weight1 weight2 weight3 weight4*	出力キューに SRR 重みを割り当てます。 デフォルトでは、4 つの重みがすべて 25 です（各キューに帯域幅の 1/4 が割り当てられています）。 *weight1 weight2 weight3 weight4* には、SRR スケジューラがパケットを送信する頻度の比率を制御する重みを入力します。各値はスペースで区切ります。指定できる範囲は 1 ～ 255 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** *interface-id* **queueing**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、出力ポートで稼動する SRR スケジューラの重みの比を設定する方法を示します。4 つのキューが使用され、共有モードの各キューに割り当てられた帯域幅は 1/（1+2+3+4）、2/（1+2+3+4）、3/（1+2+3+4）、および 4/（1+2+3+4）であり、キュー 1、2、3、および 4 に対してそれぞれ 10%、20%、30%、および 40% です。キュー 4 はキュー 1 の帯域幅の 4 倍、キュー 2 の帯域幅の 2 倍、キュー 3 の帯域幅の 1 と 1/3 倍であることを示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

出力緊急キューの設定

ポート上の出力緊急キューにある特定パケットにキューイングを行い、他のすべてのパケットに対するプライオリティを持っているかを確認できます。SRR は、他のキューの処理を行う前に、空になるまでプライオリティ キューを処理します。

出力緊急キューをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos**	スイッチ上で QoS をイネーブルにします。
ステップ 3	**interface** *interface-id*	出力ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**priority-queue out**	デフォルトではディセーブルに設定されている出力緊急キューをイネーブルにします。 このコマンドを設定すると、SRR に参加するキューは 1 つ少なくなるため、SRR 重みおよびキュー サイズの比率が影響を受けます。これは、**srr-queue bandwidth shape** 内の *weight1* または **srr-queue bandwidth shape** コマンドが無視されることを意味します（比率計算に使用されません）。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

緊急キューをディセーブルにするには、**no priority-queue out** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、SRR の重みが設定されている場合、出力緊急キューをイネーブルにする方法を示します。出力緊急キューは、設定された SRR ウェイトを上書きします。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
Switch(config-if)# end
```

出力インターフェイスの帯域幅の制限

出力ポートの帯域幅を制限できます。たとえば、カスタマーが高速リンクの一部しか費用を負担しない場合は、帯域幅をその量に制限できます。

（注）　出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合のみ、設定を変更してください。

出力ポートの出力帯域幅を制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	レートを制限するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**srr-queue bandwidth limit** *weight1*	ポートの上限となるポート速度の割合を指定します。指定できる範囲は 10 ～ 90 です。 デフォルトでは、ポートのレートは制限されず、100% に設定されています。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** [*interface-id*] **queueing**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no srr-queue bandwidth limit** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートの帯域幅を 80% に制限する例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

このコマンドを 80% に設定すると、ポートは該当期間の 20% はアイドルになります。ラインレートは接続速度の 80%（800 Mbps）に低下します。ただし、ハードウェアはライン レートが 6 つずつ増加するよう調整しているので、この値は厳密ではありません。

標準 QoS 情報の表示

Cisco IOS Release 12.2(52)SE 以降のリリースでは、表 37-15 にリストされているコマンドは、デュアル IPv4/IPv6 SDM テンプレートが使用されている場合、IPv4 および IPv6 の両方のトラフィックに適用されます。

標準 QoS 情報を表示するには、表 37-15 の特権 EXEC コマンドを 1 つ以上使用します。

表 37-15　標準 QoS 情報を表示するためのコマンド

コマンド	目的
show class-map [*class-map-name*]	トラフィックを分類するための一致条件を定義した QoS クラスマップを表示します。
show mls qos	グローバル QoS コンフィギュレーション情報を表示します。
show mls qos aggregate-policer [*aggregate-policer-name*]	集約ポリサーの設定を表示します。
show mls qos input-queue	入力キューの QoS 設定を表示します。
show mls qos interface [*interface-id*] [**buffers** | **policers** | **queueing** | **statistics**]	バッファ割り当て、ポリサーが設定されるポート、キューイング方式、入出力統計情報など、ポート レベルの QoS 情報を表示します。

表 37-15　標準 QoS 情報を表示するためのコマンド（続き）

コマンド	目的
show mls qos maps [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-mutation** *dscp-mutation-name* | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**]	QoS マッピング情報を表示します。
show mls qos queue-set [*qset-id*]	出力キューの QoS 設定を表示します。
show mls qos vlan *vlan-id*	指定された SVI に付加されたポリシー マップを表示します。
show policy-map [*policy-map-name* [**class** *class-map-name*]]	着信トラフィック クラス分類基準を定義する QoS ポリシー マップを表示します。 （注）　**show policy-map interface** 特権 EXEC コマンドを使用して、着信トラフィックの分類情報を表示しないでください。**control-plane** および **interface** キーワードは、サポートされていません。表示されている統計情報は無視してください。
show running-config | include rewrite	DSCP 透過性設定を表示します。